Τ.Ε.Ι. ΗΠΕΙΡΟΥ
T.E.I. OF EPIRUS

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ (Σ.Δ.Ο)
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ

SCHOOL OF MANAGEMENT AND ECONOMICS
DEPARTMENT OF COMMUNICATIONS, INFORMATICS AND MANAGEMENT

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Σπουδαστής:
ΖΕΡΒΟΣ ΠΑΝΑΓΙΩΤΗΣ

ΘΕΜΑ:

Ασφάλεια στο World Wide Web

ΕΙΣΗΓΗΤΗΣ: Αμαλία Γαβριήλ
Καθηγήτρια Εφαρμογών

Άρτα 2006

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος

Το World Wide Web αποτελεί τη μεγαλύτερη πηγή πληροφοριών σήμερα στον κόσμο. Το εντυπωσιακότερο ίσως στοιχείο είναι ότι εξελίσσεται με τέτοιον ιλιγγιώδη ρυθμό, ώστε να τρομάζει όσους προσπαθούν να κατανοήσουν τις τεχνολογίες που το διέπουν.

Το Internet, κάποτε ήταν προνόμιο των λίγων. Σήμερα, είναι προσιτό και διαθέσιμο στους απλούς καθημερινούς ανθρώπους, φέρνοντας στην οθόνη του υπολογιστή τους λίγη από τη μαγεία του. Το Web, ίσως είναι το πιο μαγικό κομμάτι της υπόθεσης.

Το Web αποτέλεσε και αποτελεί δέλεαρ για πολλές εταιρίες και επιχειρήσεις, που αποφάσισαν να διαφημίσουν τα προϊόντα στους στο Internet, αλλά και να τα διαπραγματευτούν. Καθημερινά πραγματοποιούνται χιλιάδες συναλλαγές, ανταλλάσσονται εμπιστευτικές πληροφορίες, παίζονται μεγάλα συμφέροντα. Μοιραία, η καινούρια αυτή πραγματικότητα προκαλεί διάφορους επιτήδειους που, είτε υποκινούμενοι από συμφέροντα είτε επειδή απλά θέλουν να διασκεδάσουν, προσπαθούν να υποκλέψουν επικοινωνίες, να καταστρέψουν δεδομένα, να ζημιώσουν επιχειρήσεις, να αποθαρρύνουν τον απλό χρήστη που θέλει και αυτός να γευθεί λίγη από τη μαγεία του διαδικτύου.

Στόχος του παρόντος είναι η αποτύπωση των συνθηκών που επικρατούν σήμερα στον ευαίσθητο τομέα της ασφάλειας των πληροφοριών στο Web, αλλά και στο Internet γενικότερα.

Στην **εισαγωγή** του παρόντος, παρουσιάζεται μια συνολική εικόνα του Internet και των υπηρεσιών του. Στο **πρώτο κεφάλαιο**, εξετάζεται η ασφάλεια στο TCP/IP μοντέλο, που αποτελεί και την "καρδιά" του Internet. Προτείνονται μηχανισμοί ασφαλείας για την προστασία των TCP/IP δικτύων και των πληροφοριών που ανταλλάσσονται μεταξύ τους. Στο **δεύτερο κεφάλαιο**, καταδεικνύεται ο ρόλος και η συνεισφορά της επιστήμης της κρυπτογραφίας στα θέματα ασφαλείας του Web. Στο **τρίτο κεφάλαιο**, περιγράφεται η λειτουργία των firewalls και ο ρόλος τους στην προάσπιση ενός δικτύου. Στο **τέταρτο κεφάλαιο**, επίκεντρο είναι η Java και η θύελλα που έχει ξεσπάσει στο Web σχετικά με το πόσο ασφαλείς ή όχι είναι οι εφαρμογές της. Ιδιαίτερη έμφαση δίνεται στα θέματα ασφαλείας που αφορούν τους browsers που ενσωματώνουν την τεχνολογία της Java, αλλά και την καινούρια τεχνολογία που έκανε την εμφάνισή της στο Web, το ActiveX. Στο **πέμπτο κεφάλαιο**, εξετάζεται η ασφάλεια του συστήματος (host), τίθενται υπ'όψην παράμετροι όπως ασφάλεια λειτουργικού συστήματος, ασφάλεια Web και FTP server, ασφάλεια Web browser, cookies, ιοί υπολογιστών.

Εισαγωγή

Τί είναι το Internet?

Internet ονομάζεται μια ομάδα παγκόσμιων πόρων πληροφοριών. Αυτοί οι πόροι (resources) έχουν τόσο μεγάλο εύρος ώστε να είναι δύσκολο να τους κατανοήσει ένα ανθρώπινο ον . Γι' αυτόν το λόγω, όχι μόνο δεν υπάρχει ούτε ένας άνθρωπος που να κατανοεί όλες τις πλευρές του Internet, αλλά δεν υπάρχει και κανένας που να γνωρίζει το μεγαλύτερο μέρος του.

Οι λεωφόροι πληροφοριών του Internet βρίσκονται σε μια μεγάλη συλλογή δικτύων υπολογιστών που ονομάζονταν Arpanet, το οποίο αναπτύχθηκε από το Υπουργείο Άμυνας των Η.Π.Α. Το αρχικό Arpanet έχει αναπτυχθεί και επεκταθεί εδώ και πολλά χρόνια, και, σήμερα, οι απόγονοί του σχηματίζουν τη ραχοκοκαλιά αυτού που ονομάζουμε Internet.

Θα ήταν λάθος να πούμε ότι το Internet είναι απλά ένα δίκτυο υπολογιστών, ή μια υπηρεσία παροχής πληροφοριών. Το Internet είναι η ζωντανή απόδειξη ότι τα ανθρώπινα όντα που έχουν την ικανότητα να επικοινωνούν μεταξύ τους χωρίς περιορισμούς και προβλήματα, επιλέγουν την κοινωνικότητα και παραμερίζουν τον εγωισμό τους.

Κάποιος θα μπορούσε να ισχυριστεί ότι ο λόγος για τον οποίο το Internet έχει τόσο μεγάλη επιτυχία είναι γιατί σ' αυτό δεν υπάρχουν ηγέτες. Όσο απίστευτο κι αν ακούγεται, δεν υπάρχει στην πραγματικότητα κάποιος που διευθύνει το Internet. Κανένας δεν είναι "υπεύθυνος", και δεν υπάρχει κάποιος οργανισμός που έχει αναλάβει το κόστος λειτουργίας του. Το Internet δεν έχει νόμους, αστυνομία ή στρατό. Δεν υπάρχουν τρόποι για να πληγώσεις κάποιον άνθρωπο. Αντίθετα, υπάρχουν πολλοί τρόποι για να δείξεις καλοσύνη. Ίσως, κάτω από τις σημερινές συνθήκες, να είναι απόλυτα φυσικό για τους ανθρώπους να μάθουν να συμβιώνουν. Για πρώτη φορά πάντως στην Ιστορία, τόσοι πολλοί άνθρωποι έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους με άνεση.

Ποιο πρωτόκολλο χρησιμοποιείται?

Η επίτευξη της λειτουργίας των υπολογιστών απαιτεί το σωστό πρωτόκολλο. Στην γλώσσα των υπολογιστών, ένα πρωτόκολλο είναι μία ομάδα συμβάσεων που καθορίζουν τον τρόπο ανταλλαγής δεδομένων μεταξύ διαφορετικών προγραμμάτων. Τα πρωτόκολλα καθορίζουν πώς μεταφέρει μηνύματα και πώς χειρίζεται τα λάθη ένα δίκτυο. Η χρήση τους επιτρέπει τη δημιουργία προδιαγραφών ανεξάρτητων από ένα συγκεκριμένο σύστημα hardware (υλικό).

Το Internet χρησιμοποιεί ένα πρωτόκολλο που ονομάζεται *TCP/IP*, από τα αρχικά των *Trasmission Control Protocol / Internet Protocol* (πρωτόκολλο ελέγχου μετάδοσης / πρωτόκολλο μεταξύ δικτύων). Το IP είναι υπεύθυνο για τη διευθυνσιοδότηση του δικτύου, ενώ το το TCP διασφαλίζει ότι τα μηνύματα θα παραδίδονται στη σωστή διεύθυνση. Αυτά τα ισχυρά πρωτόκολλα αναπτύχθηκαν το 1974 από τον Robert Kahn, ένα βασικό πρόσωπο στην ομάδα ανάπτυξης του ARPANET, και από τον επιστήμονα της Πληροφορικής Vinton G. Cerf, τέως πρόεδρο της Internet Society και αντιπρόεδρο της CNRI (Corporation for National Research Initiatives). Η ερευνητική εργασία τους δημιούργησε τους μηχανισμούς που έδωσαν τη δυνατότητα

ύπαρξης του Internet. Στην πραγματικότητα, αν θέλουμε να δώσουμε ένα σύντομο ορισμό του Internet, είναι ένα δίκτυο δικτύων που χρησιμοποιεί την ομάδα πρωτοκόλλων TCP/IP.

Το TCP/IP δεν είναι το μόνο πρωτόκολλο για τη διασύνδεση διαφορετικών δικτύων. Στην πραγματικότητα, το Internet εξελίσσεται σε ένα δίκτυο πολλαπλών πρωτοκόλλων, το οποίο ενσωματώνει και άλλες προδιαγραφές στις λειτουργίες του. Η σημαντικότερη μεταξύ αυτών είναι η Open Systems Interconnection (διασύνδεση ανοιχτών συστημάτων) ή OSI. Το OSI δημιουργημένο από τον Internetional Organisation for Standardization (διεθνής οργανισμός προτυποποίησης-ISO) έγινε ευρύτατα αποδεκτό στην Ευρώπη, όπου η τάση προς το TCP/IP ήταν μικρότερη από αυτή των Η.Π.Α. Τα συστήματα που χρησιμοποιούν άλλα πρωτόκολλα συνήθως συνδέονται στο Internet μέσω πυλών επικοινωνίας (gateways). Εντούτοις, το TCP/IP καταλαμβάνει τη μερίδα λέοντος στην μεγάλη οικογένεια πρωτοκόλλων που χρησιμοποιούνται στο διαδίκτυο.

Υπηρεσίες του Internet

Ηλεκτρονικό ταχυδρομείο (e-mail)

Ίσως η σημαντικότερη υπηρεσία στο Internet. Το ηλεκτρονικό ταχυδρομείο δίνει τη δυνατότητα αποστολής μηνυμάτων μέσω υπολογιστών. Ένα γράμμα που αποστέλλεται ηλεκτρονικά έχει τεράστια πλεονεκτήματα έναντι του συμβατικού ταχυδρομείου, ένα από τα οποία είναι η ταχύτητα παράδοσης. Ένα μήνυμα ηλεκτρονικού ταχυδρομείου μπορεί να αποθηκευτεί στον σκληρό δίσκο του υπολογιστή μας. Μπορούμε να το χειριστούμε όπως και κάθε άλλο αρχείο, φορτώνοντας το στον επεξεργαστή κειμένου για τροποποίηση και εκτύπωση. Αν θέλουμε, μπορούμε να αποθηκεύσουμε την αλληλογραφία μας ώστε να την δούμε αργότερα.

Οι διευθύνσεις e-mail των χρηστών στο Internet είναι της μορφής user@host.domain. Το ηλεκτρονικό ταχυδρομείο λειτουργεί με τη λογική client-server (πελάτης-εξυπηρετητής). Το ρόλο του server τον παίζει ένα πρωτόκολλο που διαχειρίζεται την αποστολή του μηνύματος (SMTP), ενώ το ρόλο του client παίζει το πρόγραμμα εκείνο (για Windows ή Unix) το οποίο επικοινωνεί με το SMTP (το δημοφιλέστερο πρωτόκολλο μεταφοράς μηνυμάτων) προκειμένου ο χρήστης να διαχειρίζεται μηνύματα.

Σύνδεση με απομακρυσμένο υπολογιστή (Telnet)

Το Telnet παρέχει τη δυνατότητα σύνδεσης σε έναν απομακρυσμένο υπολογιστή (remote login) και την εργασία με αυτόν σε διαλογική (interactive) βάση. Το Internet, ανοίγει το δρόμο προς ένα παγκόσμιο υπολογιστικό περιβάλλον, σε πολλούς υπολογιστές του οποίου υπάρχουν υπηρεσίες, βάσεις δεδομένων και άλλοι πόροι. Σε όλη αυτήν τη διαδικασία ο υπολογιστής που συνδέεται σε έναν απομακρυσμένο υπολογιστή συμπεριφέρεται σαν τερματικό του (του απομακρυσμένου υπολογιστή). Συνήθως, η διαδικασία σύνδεσης συνίσταται στην παροχή, από την πλευρά του χρήστη ενός User-ID (όνομα χρήστη) και ενός Password (συνθηματικό), προκειμένου να επιτευχθεί η σύνδεση. Βέβαια, υπάρχουν και ελεύθερα προσπελάσιμοι υπολογιστές, οι οποίοι είναι και η καρδιά της τόσο δημοφιλούς αυτής υπηρεσίας.

Μεταφορά αρχείων (FTP)

Το FTP ή File Transfer Protocol είναι ένας τρόπος ανταλλαγής αρχείων μεταξύ υπολογιστών. Το FTP ανήκει στην οικογένεια TCP/IP. Ένα μεγάλο πλεονέκτημα των πρωτοκόλλων του TCP/IP, είναι η παροχή μιας κοινής ομάδας εργαλείων σε υπολογιστές με διαφορετικά λειτουργικά συστήματα. Η υλοποίησή τους βοήθησε στη δημιουργία του δικτύου που ονομάζεται Internet.

Όταν επιθυμούμε να μεταφέρουμε ένα αρχείο κάποιου υπολογιστή, στον δικό μας, το πρόγραμμα ftp αναλαμβάνει την σύνδεση με τον υπολογιστή. Στη συνέχεια, όπως και με το telnet, ακολουθείται μια διαδικασία πιστοποίησης της ταυτότητάς μας, με την παροχή (από μέρους μας) όνομα χρήστη και συνθηματικού. Ακολούθως, ο απομακρυσμένος υπολογιστής, εφόσον δεχτεί να "περιηγηθούμε" στα αρχεία που διαθέτει, μας δίνει και τα σχετικά δικαιώματα ανάγνωσης- εγγραφής, που έχουν προκαθοριστεί από τον διαχειριστή του "εκεί" συστήματος. Βέβαια, υπάρχουν συλλογές αρχείων σε υπολογιστές που είναι προσπελάσιμες από όλους. Η υπηρεσία αυτή λέγεται anonymous FTP και επιτρέπει σε έναν χρήστη τη σύνδεσή του με έναν υπολογιστή, αρκεί να πληκτρολογήσει (στην προτροπή που ζητάει το συνθηματικό) την ηλεκτρονική (e-mail) διεύθυνσή του. Το anonymous FTP είναι και το "δελεαστικό" κομμάτι αυτής της υπηρεσίας.

USENET

Το USENET είναι μια μεγάλη συλλογή ομάδων συζήτησης στις οποίες μετέχουν άνθρωποι από ολόκληρο τον κόσμο. Κάθε ομάδα συζήτησης περιστρέφεται γύρω από ένα συγκεκριμένο θέμα. Το Usenet, έχει αυτή τη στιγμή περισσότερες από 10.000 ομάδες συζήτησης..

Για να διαβάσει κανείς άρθρα του USENET πρέπει να χρησιμοποιεί ένα πρόγραμμα που ονομάζεται *αναγνώστης ειδήσεων* (newsreader). Αυτό το πρόγραμμα λειτουργεί σαν διασύνδεση του χρήστη: ο χρήστης λέει ποιες ομάδες συζητήσεων θέλει να διαβάσει, και αυτό του παρουσιάζει τα άρθρα. Υπάρχουν πολλοί αναγνώστες ειδήσεων, τόσο για Unix όσο και για Windows (ιδιαίτερα μετά την είσοδο και επικράτηση στο χώρο του Internet των δημοφιλών browsers των Netscape-Microsoft, clients, τόσο για ανάγνωση νέων του USENET αλλά και για κάθε άλλη υπηρεσία, είναι ενσωματωμένοι σε αυτά τα πακέτα).

Internet Relay Chat

Το IRC (σύστημα Αναμετάδοσης Συνομιλιών του Internet) αναπτύχθηκε από το Φιλανδό Jarkko Oikarinen. Από τη στιγμή της σύλληψής του, το IRC έγινε από τους δημοφιλέστερους πόρους του Internet. Πρόκειται στην ουσία για ένα πρωτόκολλο, που επιτρέπει σε χρήστες που είναι συνδεδεμένοι στο Internet, να συνομιλούν σε πραγματικό χρόνο. Το IRC λειτουργεί σε βάση client-server. Ο χρήστης πρέπει να χρησιμοποιήσει ένα πρόγραμμα πελάτη (client), το οποίο θα συνδεθεί με ένα IRC διακομιστή (server). Όταν συνδεθεί ο client με έναν IRC server, τότε ο χρήστης μπορεί να δώσει όποια διαταγή του IRC θέλει, να συμμετάσχει σε οποιοδήποτε από τα ειδικά κανάλια συζητήσεων και να μετακινείται από το ένα κανάλι στο άλλο. Κάθε IRC server συνδέεται με άλλους, κοντινούς σε αυτόν servers. Έτσι, όλοι οι servers είναι συνδεδεμένοι μεταξύ τους και κάθε φορά που ο χρήστης έρχεται σε επαφή με το σύστημα, συνδέεται με έναν παγκόσμιο ιστό χρηστών του IRC που όλοι συνομιλούν μετάξύ τους.

Με την απότομη εξέλιξη του World Wide Web και την επικράτηση των

Microsoft Windows ως βασικό λειτουργικό σύστημα, οι δυνατότητες του IRC έχουν εξελιχτεί και αναβαθμιστεί. Έτσι, υπάρχουν γραφικοί clients που τρέχουν στα Windows, και επιτρέπουν την ταυτόχρονη σύνδεση με πολλούς IRC servers, με πολλά διαφορετικά κανάλια, όπως και την πιο φιλική για το χρήστη πλοήγηση στον χαώδη, μέχρι και πριν από μερικά χρόνια, κόσμο του IRC.

Ο Παγκόσμιος Ιστός (World Wide Web)

Ο Παγκόσμιος ιστός είναι πλέον ίσως η σημαντικότερη υπηρεσία στο Internet. Θα αναφερόμαστε σε αυτόν με τον όρο Web ή WWW. Το Web αναπτύχθηκε αρχικά στην Ελβετία, στο ερευνητικό κέντρο CERN. Ο αρχικός του σκοπός ήταν να δοθεί η δυνατότητα στους επιστήμονες του κέντρου να μοιράζονται μεταξύ τους τα διάφορα στοιχεία και να χρησιμοποιούν κοινόχρηστες πληροφορίες. Πολύ σύντομα, η ιδέα του Ιστού επεκτάθηκε σημαντικά, για να ενσωματωθεί τελικά στο Internet με τη μορφή ενός γενικού μηχανισμού για την προσπέλαση πληροφοριών και υπηρεσιών.

Το ιδανικό της ανάκτησης πληροφοριών αυτή τη στιγμή, είναι η ιδέα ενός συστήματος *υπερ-μέσων* (*hypermedia*) που θα καλύπτει όλο το φάσμα του Internet. Το Web στη σημερινή μορφή του, κάνει αυτό ακριβώς: συνιστά ένα περιβάλλον, μέσα στο οποίο επιτυγχάνεται πρόσβαση σε όλες τις μορφές δεδομένων (κείμενο, βίντεο, ήχος, εικόνα, postscript, animation), με τρόπο απόλυτα φιλικό προς τον χρήστη. Κάθε *έγγραφο υπερκειμένου* (σελίδα) στο WWW περιέχει δεδομένα ενδεχομένως κάθε είδους, αλλά και συνδέσμους σε άλλα δεδομένα. Η πλοήγηση από τον ένα σύνδεσμο στον άλλον, δικαιολογεί και την ονομασία *"Ιστός"*. Αυτό που δίνει στο Web τη μεγάλη του δύναμη είναι ότι οι σύνδεσμοί του μπορεί να οδηγήσουν σε οποιοδήποτε είδος πόρου του Internet: σε κάποιο αρχείο κειμένου, σε μια φάση εργασίας με το telnet, σε κάποια ομάδα ειδήσεων του Internet, σε ένα FTP site και πάει λέγοντας.

Κάθε πόρος στο WWW μπορεί να περιγραφεί με μια URL (*Uniform Resource Locator, Ομοιόμορφος Εντοπισμός Πόρων*) περιγραφή. Το πρώτο μέρος μιας περιγραφής (διεύθυνσης) URL αποτελούν οι χαρακτήρες http. Αυτό σημαίνει πως το έγγραφο που εμφανίζεται στην οθόνη είναι ένα αρχείο υπερκειμένου. Το όνομα http προέρχεται από τα αρχικά των λέξεων *Hypertext Transport Protocol* (*πρωτόκολλο μεταφοράς υπερκειμένου*) που είναι το πρωτόκολλο που χρησιμοποιείται στο Web για τη μεταφορά δεδομένων από το ένα μέρος στο άλλο. Στην ουσία, το WWW είναι ένα client/server σύστημα όπου ένα πρόγραμμα client που χρησιμοποιεί ο χρήστης, το οποίο ονομάζεται *φυλλομετρητής* (*browser*) αποτελεί ένα παράθυρο μέσα από το οποίο ο χρήστης "βλέπει" το Web. Από την πλευρά του Web, κάθε τι που υπάρχει στο σύμπαν αποτελείται από έγγραφα ή/και συνδέσμους (links). Μέσω του πρωτοκόλλου HTTP, ο browser διαβάζει τα δεδομένα και τους συνδέσμους που επιλέγει ο χρήστης. Αυτό που είναι ακόμα πιο σημαντικό, είναι ότι ο κάθε φυλλομετρητής ξέρει πως να προσπελάσει και WWW servers, ειδικά προγράμματα που λέγονται και δαίμονες (daemons) και προσφέρουν "δημόσια" έγγραφα υπερκειμένου. Κάθε έγγραφο υπερκειμένου, ονομάζεται *σελίδα* και είναι κατασκευασμένο με τη χρήση της γλώσσας HTML (που προήλθε από τη γλώσσα SGML, η οποία και πρωτοαναπτύχθηκε για την κατασκευή Web σελίδων). Μεγάλη σημασία στις μέρες μας αποτελεί η χρησιμοποίηση του κατάλληλου φυλλομετρητή (browser).

Σήμερα βέβαια, όπου τα περιβάλλοντα Windows σε PC's είναι τα πιο δημοφιλή , δύο browsers είναι ευρείας (σχεδόν καθολικής) χρήσης στο WWW, οι Netscape Navigator και Internet Explorer των Netscape και Microsoft αντίστοιχα , οι οποίοι εκτός από φυλλομετρητές στον Ιστό έχουν ενσωματωμένους clients για ανάγνωση e-mail, USENET news, αλλά και δημιουργία HTML σελίδων, Java.

Ασφάλεια στο TCP/IP 1

1.1 Το μοντέλο OSI

Το 1983, ο Διεθνής Οργανισμός Τυποποίησης (ISO) πρότεινε το μοντέλο αναφοράς OSI (Open Systems Interconnection, Διασύνδεση Ανοιχτών Συστημάτων) .Το μοντέλο αυτό περιγράφει τις συνδέσεις ανοικτών συστημάτων. Το OSI έχει επτά επίπεδα, τα οποία εφαρμόζουν τις ακόλουθες αρχές:

1) Ένα επίπεδο δημιουργείται εκεί όπου χρειάζεται διαφορετικός βαθμός αφαίρεσης (abstraction)

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.

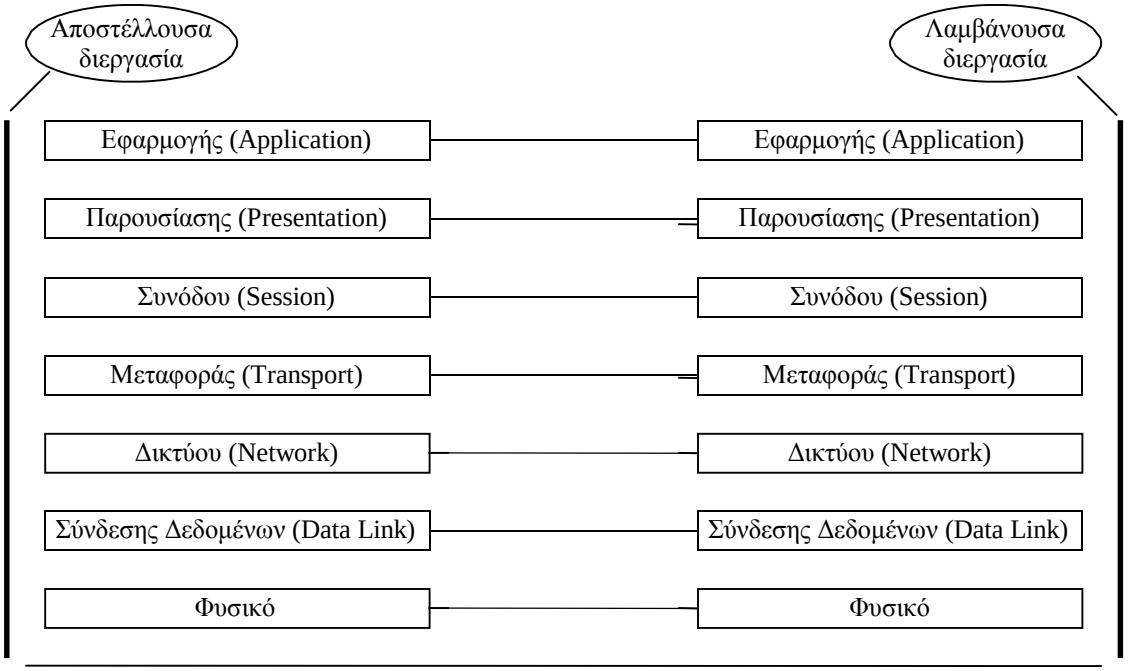
4) Η επιλογή των ορίων των επιπέδων πρέπει να γίνεται με σκοπό την ελαχιστοποίηση της ροής των πληροφοριών μέσω των διασυνδέσεων.

5) Ο αριθμός των επιπέδων θα πρέπει να είναι αρκετά μεγάλος, ώστε διακεκριμένες λειτουργίες να μην χρειάζεται να τοποθετηθούν μαζί στο ίδιο επίπεδο, χωρίς να υπάρχει τέτοια ανάγκη, και αρκετά μικρός ώστε η αρχιτεκτονική να μη γίνεται πολύπλοκη.

Κάθε επίπεδο καθορίζει μια λειτουργία επικοινωνίας δεδομένων που μπορεί να επιτελεστεί από ένα ή περισσότερα πρωτόκολλα, ενώ κάθε πρωτόκολλο επικοινωνεί με την “ομότιμη οντότητά” (peer), δηλαδή την υλοποίηση του ίδιου πρωτοκόλλου στο αντίστοιχο επίπεδο μιας διαφορετικής μηχανής.

Η μετακίνηση των δεδομένων είναι καθοδική στην αποστέλλουσα διεργασία, και ανοδική στη λαμβάνουσα διεργασία. Η αποστέλλουσα διεργασία στο σχήμα 1, διαθέτει κάποια δεδομένα, που θέλει να στείλει στη λαμβάνουσα διεργασία. Αυτή δίνει τα δεδομένα στο επίπεδο εφαρμογής, το οποίο αφού προσθέσει κάποια δικά του δεδομένα (η επικεφαλίδα, header, που μπορεί να είναι και κενή), δίνει το αποτέλεσμα στο επίπεδο παρουσίασης. Το επίπεδο παρουσίασης επεξεργάζεται με τη σειρά του τα στοιχεία, προσθέτει μια επικεφαλίδα στο μπροστινό τους μέρος, δίνοντας το αποτέλεσμα στο επίπεδο συνόδου.

Η διεργασία αυτή επαναλαμβάνεται έως ότου τα δεδομένα φτάσουν στο φυσικό επίπεδο, όπου εκεί πραγματικά, μεταδίδονται στη λαμβάνουσα μηχανή. Στη μηχανή αυτή οι διάφορες επικεφαλίδες αφαιρούνται, η μια μετά την άλλη καθώς το μήνυμα διαδίδεται προς τα επάνω έως ότου αυτό τελικά φτάσει στη λαμβάνουσα διεργασία.



Σχήμα 1 Το μοντέλο OSI

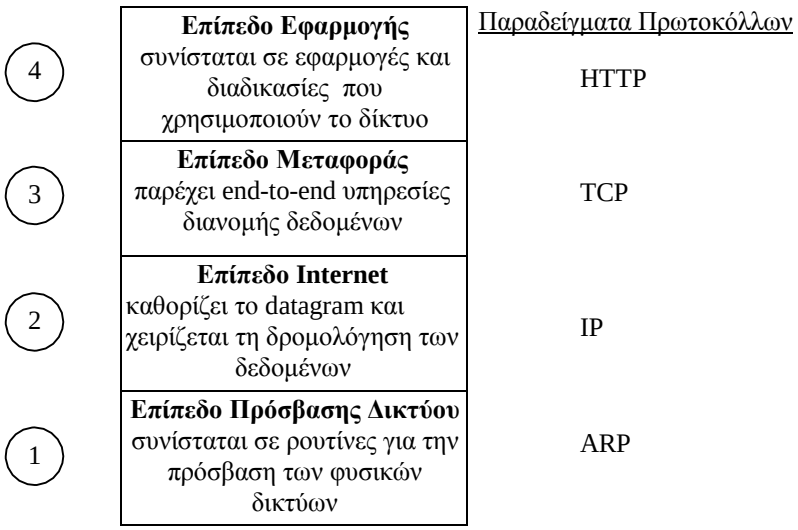
Η βασική ιδέα, είναι ότι, αν και η πραγματική μετάδοση των δεδομένων είναι κατακόρυφη, κάθε επίπεδο προγραμματίζεται σαν να ήταν στην πραγματικότητα οριζόντια. Όταν το επίπεδο μεταφοράς, για παράδειγμα, λαμβάνει ένα μήνυμα από το επίπεδο συνόδου, επισυνάπτει μια επικεφαλίδα μεταφοράς και το στέλνει στο λαμβάνων επίπεδο μεταφοράς που λαμβάνει. Από τη δική του σκοπιά, το γεγονός ότι πρέπει στην πραγματικότητα να δώσει τα δεδομένα στο επίπεδο δίκτυο, στη δική του μηχανή, είναι μια ασήμαντη τεχνική λεπτομέρεια.

1.2 Το μοντέλο TCP/IP

Ενώ δεν υπάρχει μια παγκόσμια συμφωνία σχετικά με το πώς περιγράφεται το TCP/IP με ένα μοντέλο επιπέδων, γενικά θεωρείται ότι αποτελείται από λιγότερα επίπεδα σε σύγκριση με το OSI . Όμως, η φιλοσοφία του βασίζεται σε αυτή του OSI. Στο σχήμα 2 απεικονίζεται ως ένα μοντέλο 4 επιπέδων, κάθε ένα από τα οποία επικοινωνεί με τα άλλα επίπεδα, όπως περιγράψαμε στην προηγούμενη ενότητα.

Επίπεδο "Πρόσβασης Δικτύου" (Network Access)

Το επίπεδο Πρόσβασης Δικτύου είναι το χαμηλότερο επίπεδο στην ιεραρχία των TCP/IP πρωτοκόλλων. Τα πρωτόκολλα σε αυτό το επίπεδο παρέχουν στο σύστημα τα μέσα ώστε να παραδώσει δεδομένα σε μηχανές που είναι απ'ευθείας συνδεδεμένες με το δίκτυο. Έτσι, καθορίζεται το πώς θα χρησιμοποιηθεί το δίκτυο ώστε να μεταδοθούν τα IP datagrams . Αντίθετα με τα πρωτόκολλα ανώτερων επιπέδων, τα πρωτόκολλα στο Φυσικό επίπεδο πρέπει να ξέρουν τις λεπτομέρειες του δικτύου (τη δομή του, φυσικές διευθύνσεις των μηχανημάτων κ.λ.π). Το επίπεδο αυτό συνοψίζει τις λειτουργίες των τριών τελευταίων επιπέδων του OSI (Φυσικό, Σύνδεσης Δεδομένων, Δικτύου).



Σχήμα 2 Επίπεδα στην αρχιτεκτονική των TCP/IP πρωτοκόλλων

Οι λειτουργίες που επιτελούνται σε αυτό το επίπεδο περιλαμβάνουν ενθυλάκωση (πρόσθεση επικεφαλίδας) των IP datagrams στα frames που μεταδίδονται από το δίκτυο, και η αντιστοίχηση των IP διευθύνσεων στις φυσικές διευθύνσεις που χρησιμοποιούνται από το δίκτυο.

Επίπεδο "Internet"

Το επίπεδο Internet είναι επάνω από το επίπεδο Πρόσβασης Δικτύου στην ιεραρχία των πρωτοκόλλων. Το Internet Protocol, είναι η "καρδιά" του TCP/IP και το πιο σημαντικό πρωτόκολλο στο επίπεδο Internet. Παρέχει τη βασική υπηρεσία διανομής πακέτων δεδομένων, με βάση την οποία είναι χτισμένα τα TCP/IP δίκτυα. Όλα τα πρωτόκολλα, σε όλα τα επίπεδα πάνω και κάτω από το IP, χρησιμοποιούν το Internet Protocol ώστε να μεταδώσουν δεδομένα.

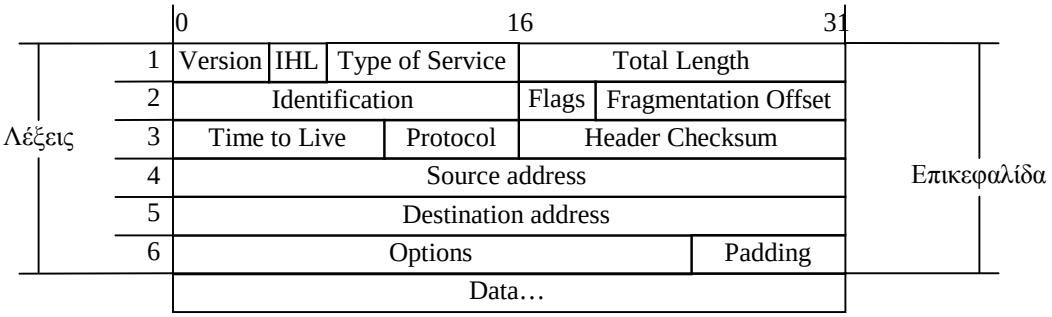
Το IP είναι *connectionless* (χωρίς σύνδεση) πρωτόκολλο. Αυτό σημαίνει ότι το IP δεν ανταλλάσσει πληροφορίες ελέγχου ώστε να εγκαταστήσει μια end-to-end σύνδεση πριν μεταδώσει τα δεδομένα. Αντίθετα, ένα *connection-oriented* (με σύνδεση) πρωτόκολλο ανταλλάσσει πληροφορίες ελέγχου με ένα απομακρυσμένο σύστημα ώστε να πιστοποιήσει ότι είναι έτοιμο να λάβει δεδομένα, πριν του τα στείλει. ¨Οταν το handshake είναι επιτυχημένο, τα συστήματα λέγεται ότι έχουν εγκαταστήσει μια σύνδεση. Το IP εμπιστεύεται άλλα επίπεδα για την εγκατάσταση της σύνδεσης.

Το datagram είναι το format πακέτου που καθορίζεται από το IP. Το σχήμα 3 αναπαριστά ένα IP datagram. Οι πρώτες πέντε από τις έξι 32-bit λέξεις του datagram, είναι πληροφορίες ελέγχου που καλούνται *"επικεφαλίδα"* (header). Εξ'ορισμού, η επικεφαλίδα έχει μήκος πέντε λέξεων. Η έκτη λέξη είναι προαιρετική. Επειδή το μήκος της μεταβλητής είναι μεταβλητό, υπάρχει ένα πεδίο που καλείται IHL, *Μήκος Επικεφαλίδας Internet* (Internet Header Length, IHL). Η επικεφαλίδα περιέχει όλες τις απαραίτητες πληροφορίες, ώστε να παραδοθεί το πακέτο στον προορισμό του.

Το IP παραδίδει το datagram ελέγχοντας τη *Διεύθυνση Προορισμού* (Destination Address) στην λέξη 5 της επικεφαλίδας. Εάν η Διεύθυνση Προορισμού ανήκει στο τοπικό δίκτυο, το πακέτο παραδίδεται απευθείας στον προορισμό του. Αν δεν ανήκει στο

τοπικό δίκτυο, το πακέτο προωθείται στον *δρομολογητή* για να αναλάβει αυτός την παράδοση.

Όταν το IP λαμβάνει ένα datagram το οποίο έχει τη διεύθυνση του τοπικού host, πρέπει να περάσει το τμήμα δεδομένων (data portion) του datagram στο σωστό πρωτόκολλο επιπέδου Μεταφοράς. Αυτό γίνεται χρησιμοποιώντας τον *Αριθμό Πρωτοκόλλου* (Protocol Number) από τη λέξη 3 της επικεφαλίδας. Κάθε πρωτόκολλο επιπέδου Μεταφοράς έχει ένα μοναδικό Αριθμό Πρωτοκόλλου, ως προς το IP.

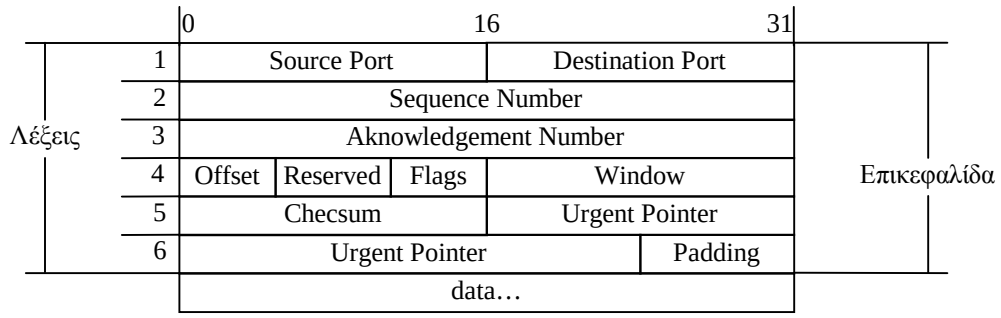


Σχήμα 3 Το format του IP datagram

Επίπεδο "Μεταφοράς" (Transport)

Πάνω από το επίπεδο Internet βρίσκεται το επίπεδο Μεταφοράς. Τα δύο σημαντικότερα πρωτόκολλα αυτού του επιπέδου είναι το **TCP** (Transmission Control Protocol) και το **UDP** (User Datagram Protocol). Το TCP προσφέρει *αξιόπιστες* (reliable) υπηρεσίες παράδοσης δεδομένων με end-to-end ανίχνευση και διόρθωση λαθών. Το UDP προσφέρει connectionless, χαμηλού φόρτου (low-overhead), αναξιόπιστες υπηρεσίες παράδοσης δεδομένων. Λέγοντας αξιόπιστη υπηρεσία, εννοούμε ότι υπάρχουν εγγενείς τεχνικές στο πρωτόκολλο ώστε να πιστοποιεί ότι τα δεδομένα έχουν φτάσει σωστά στο δίκτυο.

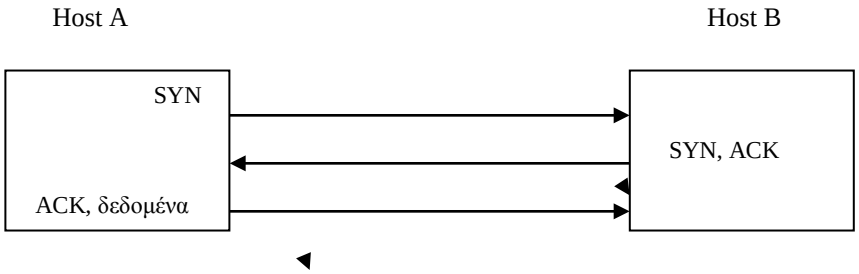
Το TCP προσφέρει αξιοπιστία με έναν μηχανισμό που καλείται PAR (Positive Aknowledgment with Retransmission). Με απλά λόγια, ένα σύστημα που χρησιμοποιεί το PAR στέλνει εκ νέου τα δεδομένα, εκτός και αν "ακούσει" από το απομακρυσμένο σύστημα ότι τα δεδομένα έφθασαν κανονικά. Η μονάδα δεδομένων που ανταλλάσετε μεταξύ συνεργαζόμενων TCP modules καλείται **segment** (σχήμα 4). Κάθε segment περιέχει ένα checksum το οποίο χρησιμοποιεί ο παραλήπτης ώστε να πιστοποιήσει ότι τα δεδομένα είναι απαράλλαχτα. Εαν το segment δεδομένων λαμβάνεται χωρίς να έχει υποστεί αλλαγές, ο παραλήπτης στέλνει ένα μήνυμα Θετικής Επιβεβαίωσης (Positive Acknowledgment) πίσω στον αποστολέα. Εάν τα δεδομένα έχουν παραβιαστεί, ο παραλήπτης τα απαλλάσσει (discard). Μετά από μια λογική περίοδο διαλλείματος (time- out), ο αποστολέας ξανά-στέλνει το TCP-module για το οποίο δεν έλαβε θετική επιβεβαίωση.



Σχήμα 4 Το format του TCP segment

Το TCP είναι connection-oriented. Εγκαθιστά μια λογική end-to-end σύνδεση μεταξύ δύο επικοινωνούντων hosts. Πληροφορίες ελέγχου που καλούνται handshake (χειραψία), ανταλλάσσονται μεταξύ των δύο μηχανημάτων ώστε να ολοκληρωθεί ένας "διάλογος" προτού αρχίσουν να μεταδίδονται τα δεδομένα. Το TCP προσδιορίζει την λειτουργία ελέγχου ενός segment μεταβάλλοντας το αντίστοιχο bit στο πεδίο *Flags* (σημαίες) στη λέξη 4 της επικεφαλίδας του segment.

Ο τύπος του handshake που χρησιμοποιείται από το TCP καλείται *three way handshake* (τριπλή χειραψία), επειδή ανταλλάσσονται τρία segments. Το σχήμα 5 δείχνει την απλούστερη μορφή μιας *τριπλής χειραψίας*. Ο host A αρχίζει τη σύνδεση στέλνοντας στον host B ένα segment με το bit **SYN** (Synchronize sequence numbers) αληθές. Αυτό το segment λέει στον host B ότι ο A θέλει να αρχίσει μια σύνδεση, και επίσης λέει στον B ποιον *αριθμό ακουλουθίας* (**sequence number**) θα χρησιμοποιήσει ο host A ως τον αρχικό αριθμό για τα segments του. (Οι *αριθμοί ακολουθίας* χρησιμοποιούνται ώστε να κρατούν τα δεδομένα στη σωστή σειρά). Ο host B απαντάει στον A με ένα segment το οποίο έχει αληθή τα ACK (Acknowledgment) και SYN bits. Το segment του B *επιβεβαιώνει* (acknowledges) τη λήψη του segment του A, και πληροφορεί τον A για τον *αριθμό ακολουθίας* με τον οποίο θα αρχίσει ο B. Τέλος, ο A στέλνει ένα segment που επιβεβαιώνει τη λήψη του segment του B, και μεταφέρει τα πρώτα ουσιαστικά δεδομένα.



Σχήμα 5 Τριπλή χειραψία (three-way handshake)

Το TCP standard δεν απαιτεί κάθε σύστημα να αρχίζει να απαριθμεί τα bytes με ένα συγκεκριμένο αριθμό. Αντίθετα, κάθε σύστημα επιλέγει τον αριθμό που θα χρησιμοποιήσει ως σημείο εκκίνησης. Προκειμένου να παρακολουθεί τη ροή των δεδομένων, κάθε σύστημα πρέπει να ξέρει τον *αρχικό αριθμό* του άλλου. Έτσι, τα δύο συστήματα ανταλλάσουν SYN segments κατά τη διάρκεια της *χειραψίας*. Το πεδίο "Αριθμός Ακολουθίας" (Sequence Number) στο SYN segment (σχήμα 4) περιέχει τον

Αρχικό Αριθμό Ακολουθίας (**Initial Sequence Number**) ISN, ο οποίος είναι και το σημείο εκκίνησης για κάθε σύστημα. Το ISN είναι συνήθως 0, παρότι αυτό δε ζητείται από το πρωτόκολλο.

Το segment Επιβεβαίωσης (Acknowledgment, ACK) επιτελεί δυο λειτουργίες: *θετική επιβεβαίωση* (positive acknowledgment) και *έλεγχο ροής* (flow control). Η *επιβεβαίωση* λέει στον αποστολέα πόσα δεδομένα έχουν ληφθεί, και πόσα ακόμα μπορεί να δεχθεί ο παραλήπτης. Ο *Αριθμός Επιβεβαίωσης* (Acknowledgment Number) είναι ο αριθμός ακολουθίας του τελευταίου byte που ελήφθη. Το standard δεν απαιτεί επιβεβαίωση για κάθε πακέτο. Ο *Αριθμός Επιβεβαίωσης* είναι μια θετική επιβεβαίωση για όλα τα bytes, μέχρι αυτόν τον αριθμό. Για παράδειγμα, εάν το πρώτο byte που στάλθηκε ήταν αριθμημένο ως 1 και έχουν ήδη ληφθεί με επιτυχία 2000 bytes, τότε ο *Αριθμός Επιβεβαίωσης* θα είναι ίσος με 2000.

Το πεδίο **Window** (Παράθυρο) περιέχει τον αριθμό των bytes που το απομακρυσμένο σύστημα είναι ικανό να δεχθεί. Προσδιορίζει στον παραλήπτη ότι μπορεί να συνεχίσει να στέλνει segments, αρκεί ο συνολικός αριθμός των bytes που στέλνει να είναι μικρότερος από την τιμή του window.

Επίπεδο "Εφαρμογής" (Application)

Αυτό το επίπεδο περιλαμβάνει όλες τις διαδικασίες που χρησιμοποιούν τα πρωτόκολλα του επιπέδου Μεταφοράς (Transport) προκειμένου να μεταδώσουν δεδομένα. Υπάρχουν πολλά πρωτόκολλα εφαρμογής. Τα περισσότερα παρέχουν υπηρεσίες χρήστη, ενώ καινούριες υπηρεσίες προστίθενται συνεχώς στο επίπεδο αυτό. Τα πιο ευρέως γνωστά πρωτόκολλα εφαρμογής είναι:

- TELNET (Network Terminal Protocol): παρέχει απομακρυσμένη σύνδεση μέσω του δικτύου.
- FTP (File Transfer Protocol): χρησιμοποιείται για αλληλεπιδραστική (interactive) μεταφορά αρχείων.
- SMTP (Simple Mail Transfer Protocol): παραδίδει ηλεκτρονική αλληλογραφία (mail).
- DNS (Domain Name Service): αντιστοιχεί IP διευθύνσεις με ονόματα hosts.
- RIP (Routing Information Protocol): χρησιμοποιείται από υπολογιστές του δικτύου για ανταλλαγή πληροφοριών δρομολόγησης.
- NFS (Network File System): επιτρέπει σε αρχεία να "μοιράζονται" μεταξύ πολλών hosts στο δίκτυο.

Παραδίδοντας τα δεδομένα

Προκειμένου να παραδοθούν δεδομένα μεταξύ δύο Internet hosts, είναι αναγκαίο να μετακινηθούν τα δεδομένα μέσω του δικτύου στο σωστό host, και μέσα στο host αυτόν, στο σωστό χρήστη ή διαδικασία. Το TCP/IP χρησιμοποιεί τρία "σχήματα" προκειμένου να πραγματοποιήσει αυτήν την εργασία:

Διευθυνσιοδότηση (Addressing): IP διευθύνσεις, που προσδιορίζουν μοναδικά κάθε host στο Internet, εξασφαλίζουν την παράδοση των δεδομένων στο σωστό host.

Δρομολόγηση (Routing): Gateways παραδίδουν δεδομένα στο σωστό δίκτυο.
Πολύπλεξη (Multiplexing): Πρωτόκολλα και αριθμοί θυρών (port numbers) παραδίδουν δεδομένα στο κατάλληλο λογισμικό μέσα στο host

Διευθυνσιοδότηση στο Internet

Το Internet Protocol κινεί δεδομένα μεταξύ hosts, με την μορφή datagrams. Κάθε datagram παραδίδεται στη διεύθυνση η οποία περιέχεται στο Destination Address (διεύθυνση παραλήπτη) της επικεφαλίδας του datagram. Η Destination Address είναι μία 32-bit IP διεύθυνση που περιέχει αρκετή πληροφορία ώστε να ονοματίσει μοναδικά ένα δίκτυο και ένα συγκεκριμένο host σε αυτό το δίκτυο.

Μία IP διεύθυνση περιέχει ένα *τμήμα δικτύου* και ένα *τμήμα host.* Ο αριθμός των bits που χρησιμοποιούνται για να αναπαριστούν τα δύο τμήματα, ποικίλλει ανάλογα με την *τάξη* της διεύθυνσης. Οι τέσσερις τάξεις διευθύνσεων είναι οι A, B, C, D. Το IP χρησιμοποιεί κάποιους κανόνες, προκειμένου να προσδιορίσει σε ποια τάξη ανήκει μια διεύθυνση:

- Αν το πρώτο bit μιας IP διεύθυνσης είναι 0, τότε πρόκειται για διεύθυνση δικτύου τάξης A. Το πρώτο bit μιας A διεύθυνσης ονοματίζει την τάξη της διεύθυνσης. Τα επόμενα 7 bits ονοματίζουν το δίκτυο, και τα τελευταία 24 bits ονοματίζουν το host.
- Αν τα πρώτα δύο bits της διεύθυνσης είναι 1 0, τότε πρόκειται για διεύθυνση δικτύου τάξης B. Τα πρώτα δύο bits καθορίζουν την τάξη, τα επόμενα 14 bits καθορίζουν το δίκτυο, και τα τελευταία 16 καθορίζουν το host.
- Αν τα πρώτα τρία bits της διεύθυνσης είναι 1 1 0, τότε πρόκειται για μια διεύθυνση δικτύου τάξης C. Σε μια διεύθυνση C τάξης, τα πρώτα τρία bits καθορίζουν την τάξη. Τα επόμενα 21 bits καθορίζουν τη διεύθυνση δικτύου, και τα τελευταία 8 bits ονοματίζουν το host.
- Αν τα πρώτα τρία bits της διεύθυνσης είναι 1 1 1, τότε πρόκειται για μία ειδική διεύθυνση, που λέγεται διεύθυνση τάξης D. Οι διευθύνσεις αυτού του τύπου λέγονται διευθύνσεις multicast (πολυμετάδοσης) και χρησιμοποιούνται για την ταυτόχρονη διευθυνσιοδότηση ομάδων υπολογιστών (σήμερα, οι διευθύνσεις αυτού του τύπου χρησιμοποιούνται ευρέως σε εφαρμογές όπως το video conferencing κ.α)

Το IP χρησιμοποιεί το *τμήμα δικτύου* της διεύθυνσης προκειμένου να δρομολογήσει το datagram ανάμεσα στα δίκτυα. Η πλήρης διεύθυνση, συμπεριλαμβανομένου και του *τμήματος host,* χρησιμοποιείται για την τελική παράδοση, όταν το datagram φθάσει στο δίκτυο προορισμού.

Δεν είναι διαθέσιμες για χρήση όλες οι διευθύνσεις δικτύων ή host. Για παράδειγμα, οι διευθύνσεις με το πρώτο byte να παίρνει τιμές μεγαλύτερες από το 223, ανήκουν σε αυτήν την κατηγορία, όπως και οι A διευθύνσεις 0 και 127 που χρησιμοποιούνται για ειδικούς σκοπούς, που ξεφεύγουν από τους στόχους του κεφαλαίου αυτού.

Ουσιαστικά, μία IP διεύθυνση αντιστοιχεί σε μία διασύνδεση (interface) δικτύου, και όχι απαραίτητα σε έναν υπολογιστή. Δηλαδή, ένας host που έχει δύο διασυνδέσεις δικτύου, μία Ethernet και μία token ring διασύνδεση, θα έχει και δύο IP διευθύνσεις.

Η δομή μιας IP διεύθυνσης μπορεί να τροποποιηθεί χρησιμοποιώντας τα bits διεύθυνσης host (host address bits) ως επιπλέον bits διεύθυνσης δικτύου (network address bits). Με τη χρήση μιας ειδικά δεσμευμένης διεύθυνσης, η "διαχωριστική γραμμή" μεταξύ των network address bits και host address bits μετακινείται, δημιουργώντας επιπλέον διευθύνσεις δικτύων (άρα θεωρητικά και επιπλέον δίκτυα) στην IP διεύθυνση. Τα δίκτυα αυτά λέγονται *υποδίκτυα (subnets).*

Αρχιτεκτονική δρομολόγησης στο Internet.

Η ιεραρχία των gateways στο Internet αντανακλά την ιστορία του Internet, το οποίο και "χτίστηκε" επάνω στο ARPANET. Όταν το Internet δημιουργήθηκε, το ARPANET ήταν η ραχοκοκκαλιά του δικτύου: ένα κεντρικό μέσο αναλάμβανε την

μεταφορά δεδομένων σε μεγάλη απόσταση. Το κεντρικό αυτό μέσο ονομάζονταν *πυρήνας (Core)* και τα κεντρικώς διαχειριζόμενα gateways που το διασύνδεαν ονομάζονταν *core gateways*. Όταν χρησιμοποιείται η ιεραρχική αυτή δομή, οι πληροφορίες δρομολόγησης (routing information) για όλα τα δίκτυα μεταβιβάζονται στα core gateways. Αυτά, επεξεργάζονται τις πληροφορίες αυτές και τις ανταλλάσσουν μεταξύ τους χρησιμοποιώντας το πρωτόκολλο GGP (Gateway to Gateway Protocol). Οι επεξεργασμένες αυτές πληροφορίες στη συνέχεια μεταβιβάζονται στα εξωτερικά gateways.

Έξω από το Internet core, υπάρχουν ομάδες ανεξάρτητων δικτύων που ονομάζονται *αυτόνομα συστήματα (autonomous systems, AS)*. Ένα αυτόνομο σύστημα μπορεί να είναι μια συλλογή δικτύων και gateways με το δικό της εσωτερικό μηχανισμό συγκέντρωσης πληροφοριών δρομολόγησης και μεταβίβασής των σε άλλα ανεξάρτητα δίκτυα. Οι πληροφορίες δρομολόγησης που μεταβιβάζονται σε άλλο αυτόνομο σύστημα καλούνται *πληροφορίες προσέγγισιμότητας (reachability information)*. Η πληροφορία προσέγγισιμότητας, λέει απλά ποια δίκτυα μπορούν να προσεγγιστούν μέσω του συγκεκριμένου AS. Πρωτόκολλα όπως το EGP (Exterior Gateway Protocol) και προσφάτως το BGP (Border Gateway Protocol), χρησιμοποιούνται για την μεταβίβαση πληροφοριών προσεγγισιμότητας μεταξύ AS.

Τα gateways δρομολογούν δεδομένα μεταξύ δικτύων. Όλα όμως τα συστήματα σε ένα δίκτυο, από τις πύλες (gateways) έως τους hosts, πρέπει να παίρνουν αποφάσεις δρομολόγησης. Για τους περισσότερους hosts, οι αποφάσεις δρομολόγησης είναι απλές:

- Εαν ο host προορισμού είναι στο τοπικό δίκτυο, τα δεδομένα παραδίδονται στο host προορισμού.
- Εάν ο host προορισμού είναι σε ένα απομακρυσμένο δίκτυο, τα δεδομένα προωθούνται σε ένα τοπικό gateway (router).

Το IP παίρνει αποφάσεις δρομολόγησης με βάση το τμήμα δικτύου της διεύθυνσης προορισμού, κοιτάζοντας "υψηλότερα" bits της διεύθυνσης προκειμένου να καθορίσει το δίκτυο προορισμού. Αφού το καθορίσει, τότε αναζητεί πληροφορίες στον τοπικό *πίνακα δρομολόγησης (routing table)*. Ο πίνακας δρομολόγησης μπορεί να δημιουργηθεί από τον διαχειριστή του συστήματος ή με τη βοήθεια πρωτοκόλλων δρομολόγησης, όπως το RIP (Routing Information Protocoll) και προσφάτως το OSPF (Open Shortest Path First) πρωτόκολλο.

Η IP διεύθυνση και ο πίνακας δρομολόγησης κατευθύνουν ένα datagram σε ένα συγκεκριμένο φυσικό δίκτυο, αλλά όταν δεδομένα ταξιδεύουν μέσω ενός δικτύου, πρέπει να υπακούουν στα πρωτόκολλα φυσικού επιπέδου που χρησιμοποιούνται από αυτό το δίκτυο. Τα φυσικά δίκτυα έχουν τα δικά τους συστήματα διευθυνσιοδότησης, και υπάρχουν τόσες κατηγορίες διευθύνσεων όσα και τα ήδη των φυσικών δικτύων. Μια "δουλειά " για τα πρωτόκολλα στο επίπεδο πρόσβασης δικτύου είναι η μετατροπή IP διευθύνσεων σε διευθύνσεις φυσικού δικτύου. Τυπικό παράδειγμα είναι η μετατροπή IP διευθύνσεων σε Ethernet διευθύνσεις. Το πρωτόκολλο που πραγματοποιεί τη λειτουργία αυτή είναι το ARP (Address Resolution Protocol). Αντίθετα, για τη μετατροπή Ethernet διευθύνσεων σε IP διευθύνσεις χρησιμοποιείται το RARP (Reverse Address Protocol.

Πρωτόκολλα, θύρες και sockets

Καθώς τα δεδομένα δρομολογούνται μέσα από το δίκτυο και παραδίδονται στο συγκεκριμένο host, πρέπει να παραδοθούν και στο σωστό χρήστη και διαδικασία. Καθώς τα δεδομένα κινούνται προς τα επάνω ή προς τα κάτω, στα επίπεδα του TCP/IP, είναι απαραίτητη η ύπαρξη ενός μηχανισμού που θα τα παραδώσει στα σωστά πρωτόκολλα,

για κάθε επίπεδο. Το σύστημα πρέπει να είναι ικανό να συνθέσει δεδομένα από πολλές εφαρμογές σε λίγα πρωτόκολλα μεταφοράς, και από τα πρωτόκολλα μεταφοράς στο Internet Protocol. Η σύνδεση πολλών πηγών δεδομένων σε μια ροή δεδομένων καλείται *πολύπλεξη* (*multiplexing*). Δεδομένα που φθάνουν στο δίκτυο πρέπει να *αποπλεχθούν* (*demultiplexing*): να διαιρεθούν δηλαδή για παράδοση σε πολλαπλές διαδικασίες. Προκειμένου να γίνει αυτό, το IP χρησιμοποιεί *protocol numbers (αριθμούς πρωτοκόλλων)* για να προσδιορίσει τα πρωτόκολλα μεταφοράς, και τα πρωτόκολλα μεταφοράς χρησιμοποιούν *port numbers (αριθμούς θυρών)* για να προσδιορίσουν εφαρμογές. Ο συνδυασμός μιας IP διεύθυνσης και ενός port number καλείται *socket*.

1.3 Προβλήματα ασφαλείας στο TCP/IP

Τα προβλήματα ασφαλείας που αντιμετωπίζει ένα TCP/IP δίκτυο είναι πολλά, και η ομαδοποίηση τους είναι συχνά δύσκολη, Εντούτοις, αξίζει να αναφερθούμε σε ορισμένα προβλήματα τα οποία απασχόλησαν και απασχολούν κατά καιρούς τους διαχειριστές συστημάτων, αλλά και τους απλούς χρήστες των hosts ενός TCP/IP δικτύου.

1.3.1 Επιθέσεις Άρνησης Υπηρεσίας (Denial Of Service)

Οι επιθέσεις αυτού του είδους έχουν ως σκοπό την μείωση ή την εξάλειψη της ικανότητας ενός συστήματος να προσφέρει τις υπηρεσίες του στους νόμιμους χρήστες. Χαρακτηριστικότερες είναι οι TCP SYN Flooding επιθέσεις, οι επιθέσεις με το γνωστό πρόγραμμα Ping, και οι επιθέσεις με τη χρήση του UDP. Συνήθως, η δυσλειτουργία διατηρείται και για ένα αρκετά μεγάλο χρονικό διάστημα μετά το πέρας της επίθεσης.

1.3.1.1 TCP SYN Flooding

Η επίθεση TCP SYN Flooding (“Πλυμμήρισμα με SYN πακέτα”) έχει ως αποτέλεσμα την μη ανταπόκριση των servers σε αιτήσεις για νέες συνδέσεις από clients. Η επίθεση αυτή εκμεταλλεύεται τον τρόπο με τον οποίο το TCP πρωτόκολλο εγκαθιστά μια νέα σύνδεση. Κάθε φορά που ένας client, όπως ο Netscape browser, επιχειρεί να αρχίσει μια σύνδεση με έναν server, κάποιες πληροφορίες αποθηκεύονται στον server. Επειδή η πληροφορία που αποθηκεύεται, απασχολεί τη μνήμη και τους υπολογιστικούς πόρους του συστήματος, μόνο έναςπεριορισμένοςαριθμός εξελισσόμενων συνδέσεων επιτρέπεται, και αυτός ο αριθμός είναι συνήθως μικρότερος του δέκα.

Ας συγκεκριμενοποιήσουμε την επίθεση, χρησιμοποιώντας την ορολογία του TCP πρωτοκόλλου. Μια TCP σύνδεση αρχικοποιείται όταν ο client στέλνει στον server ένα TCP segment με το SYN bit της επικεφαλίδας αληθές, όπως έχουμε πει. Κανονικά, ο server στέλνει ένα SYN/ACK πίσω στον client, η διεύθυνση του οποίου δηλώνεται στο 32-bit πεδίο “Διεύθυνση Πηγής” (Source Adress) στην IP επικεφαλίδα. Ο client στη συνέχεια, στέλνει ένα ACK στον server, και η μεταφορά δεδομένων μπορεί να αρχίσει. Το όριο των εξελισσόμενων συνδέσεων (SYN αιτήσεις) που μπορεί να επεξεργαστεί το TCP για ένα ένα συγκεκριμένο socket, καλείται “backlog, και είναι το μέγεθος της ουράς όπου κρατούνται οι εισερχόμενες (αλλά ατελείς) συνδέσεις. Εαν ξεπεραστεί αυτό το όριο, το TCP απορρίπτει σιωπηλά όλες τις SYN αιτήσεις, μέχρι να μπορέσει να χειριστεί τις συνδέσεις που εκκρεμούν.

Κατ’αυτόν τον τρόπο, η δομή δεδομένων (ουρά) ή πίνακας που ο server χρησιμοποιεί ώστε να περιγράψει όλες τις εκκρεμείς συνδέσεις, υπερχειλίζεται , καθώς είναι πεπερασμένου μεγέθους. Έτσι, το σύστημα είναι ανήμπορο να δεχθεί νέες εισερχόμενες συνδέσεις, μέχρις ότου αδειάσει ο πίνακας. Κανονικά, υπάρχει μια συγκεκριμένη χρονική περίοδος που καλείται time-out (διάλλειμα), μετά το πέρας της οποίας όλες οι εκκρεμείς συνδέσεις εκπνέουν, οπότε και ο server επανέρχεται στην κανονική του λειτουργία και είναι ικανός να ξανά-δεχθεί καινούριες αιτήσεις για σύνδεση. Παρ’όλα αυτά, ο επιτιθέμενος host ενδέχεται να εξακολουθήσει να στέλνει IP

πακέτα με αλλαγμένη διεύθυνση (spoofed), τα οποία αφενός θα ζητούν καινούρια σύνδεση και αφετέρου θα αποστέλλονται με γρηγορότερο ρυθμό από αυτόν που χρησιμοποιείται ώστε να εκπνέουν οι εκκρεμείς συνδέσεις..

Στις περισσότερες περιπτώσεις, τα θύματα αυτής της επίθεσης δεν μπορούν να δεχθούν εισερχόμενες συνδέσεις. Εντούτοις, η επίθεση δεν επηρεάζει τις ήδη υπάρχουσες εισερχόμενες συνδέσεις (για τις οποίες έχει γίνει τριπλό handshake), όπως επίσης δεν επηρεάζει και τις εξερχόμενες συνδέσεις, δηλαδή τις συνδέσεις που αρχικοποιούνται από τον server που δέχεται την επίθεση. Βέβαια, σε ορισμένες περιπτώσεις το σύστημα έχει τόσο μεγάλη απώλεια μνήμης και υπολογιστικών πόρων, που ενδέχεται να καταρρεύσει εντελώς

Το σημείο από όπου εξαπολύεται η επίθεση, δεν είναι εύκολο να εντοπιστεί, εφόσον οι διευθύνσεις πηγής (source address) στα SYN πακέτα είναι παραλλαγμένες. Όταν το πακέτο φθάνει στο server σύστημα του θύματος, δεν υπάρχει τρόπος να καθοριστεί η πραγματική διεύθυνση πηγής.

Οι χρήστες του συστήματος που δέχεται την επίθεση, μπορεί να μην αντιληφθούν την επίθεση, καθώς τα "ψεύτικα" (spoofed) IP πακέτα μπορεί να φορτώνουν πολύ το σύστημα. Όμως οι clients που προσπαθούν να συνδεθούν στο σύστημα, θα έχουν πρόβλημα. Οι administrators μπορούν να διαπιστώσουν την εξέλιξη της επίθεσης, ελέγχοντας την κατάσταση της κίνησης στο server σύστημα.

Λύση πρώτη: Φιλτράρισμα

Εφόσον το δίκτυο προωθεί τα πακέτα με βάση τη διεύθυνση προορισμού τους, ο μόνος τρόπος πιστοποίησης της προέλευσης ενός πακέτου, είναι η χρησιμοποίηση φιλτραρίσματος της εισόδου με βάση την πηγή, διαμορφώνοντας κατάλληλα τους δρομολογητές του δικτύου ή χρησιμοποιώντας firewalls. Έτσι, είναι απαραίτητο αφενός ένα φίλτρο το οποίο δε θα επιτρέπει εισερχόμενα (στο εξωτερικό interface του δρομολογητή) που θα έχουν διεύθυνση πηγής κάποια από το εσωτερικό δίκτυο, αφετέρου ένα φίλτρο το οποίο δε θα επιτρέπει εξερχόμενα (στο εσωτερικό interface του δρομολογητή) τα οποία έχουν διεύθυνση πηγής διαφορετική από όλες τις διευθύνσεις του εσωτερικού δικτύου.

Ο συνδυασμός των δύο αυτών φίλτρων θα αποτρέψει τους επιτιθέμενους εκτός δικτύου από το να στείλουν πακέτα που προέρχονται δήθεν από το εσωτερικό δίκτυο (φίλτρο 1), όπως επίσης και θα αποτρέψει τους χρήστες εντός δικτύου από το να στείλουν πακέτα που προέρχονται δήθεν από hosts εκτός δικτύου (φίλτρο 2). Βέβαια, είναι προφανές ότι αυτά τα μέτρα δεν εξαλείφουν τις πιθανότητες μιας TCP SYN επίθεσης, απλά περιορίζουν τις μορφές που μπορεί να πάρει αυτή η επίθεση. Οι ISPs που παρέχουν υπηρεσίες Internet μπορούν να τοποθετήσουν φίλτρα στους δρομολογητές για λογαριασμό των χρηστών που το επιθυμούν.

Λύση δεύτερη: Το μέγεθος της ουράς και το time-out

Παρότι ορισμένοι έχουν περιγράψει την TCP SYN επίθεση ως "λάθος" (bug) στην υλοποίηση του TCP/IP , το σωστό είναι ότι πρόκειται απλά για ένα "χαρακτηριστικό" του σχεδιασμού του. Το TCP/IP σχεδιάστηκε για ένα "φιλικό" Internet, και η περιορισμένου μεγέθους ουρά για την οποία μιλήσαμε νωρίτερα λειτουργούσε κανονικά για πολλά χρόνια.

Ορισμένοι έχουν προτείνει την αύξηση του μεγέθους της ουράς και τη μείωση της τιμής του time-out. Όπως είπαμε, η τιμή του time-out καθορίζει το "πόσο χρόνο διατηρείται μια είσοδος στην ουρα, μέχρις ότου να ληφθεί ένα ACK". Το πρόβλημα της αύξησης του μεγέθους της ουράς είναι ότι στην πραγματικότητα υπάρχουν πολλές ουρές (μία για κάθε TCP server στο σύστημα -HTTP, FTP, SMTP κ.λ.π), οπότε μεγαλώνοντας τις ουρές σε ένα μέγεθος της τάξης, για παράδειγμα, των 8 Kilobytes, θα είχε ως

αποτέλεσμα το λειτουργικό σύστημα να απαιτεί μεγάλες ποσότητες μνήμης.

Η μείωση των time-outs, όταν συνδυαστεί με μεγαλύτερες ουρές, βοηθάει υπό την έννοια ότι τα "ψεύτικα" (spoofed) πακέτα αφαιρούνται από τις ουρές πολύ γρήγορα. Βέβαια, η μείωση του time-out θα επηρρέαζε αρνητικά τους απομακρυσμένους χρήστες οι οποίοι έχουν αργή σύνδεση στο Internet, και οι οποίοι δε θα είχαν έτσι τη δυνατότητα να συνδεθούν με τον server, αφού το σύστημα θα τους αντιμετώπιζε ως προπομπούς μιας TCP SYN επίθεσης άρνησης υπηρεσίας.

Γενικά θα λέγαμε ότι μια βιώσιμη λύση θα ήταν ο επαναχεδιασμός της υλοποίησης του TCP/IP. Εάν ήταν δυνατή η αύξηση του μεγέθους της ουράς χωρίς να απαιτείται πολλή μνήμη, τότε δεν θα υφίστατο το πρόβλημα. Επίσης, μια διαφορετική υλοποίηση του IP, σύμφωνα με την οποία θα ήταν δυνατός ο εντοπισμός της αληθινής IP διεύθυνσης ενός εισερχόμενου πακέτου, θα αποτελούσε ένα βήμα προς τη σωστή κατεύθυνση.

1.3.1.2 Επίθεση με Ping

Τα Ping πακέτα αποτελούν ένα μεγάλο τμήμα των πακέτων που κυκλοφορούν σε ένα TCP/IP δίκτυο. Έχουν ένα standard format το οποίο αναγνωρίζεται από κάθε "IP-ομιλών" δρομολογητή, και χρησιμοποιούνται διεθνώς για διαχείριση και έλεγχο του δικτύου. Έτσι, οι διαχειριστές πολλές φορές ρυθμίζουν τα firewalls ώστε να επιτρέπουν την έλευση ping πακέτων. Τα Ping πακέτα ονομάζονται συνήθως ICMP_ECHO πακέτα.

Το Internet Control Mesage protocol αποτελεί πρωτόκολλο του επιπέδου Internet. Είναι ένα connectionless πρωτόκολλο το οποίο χρησιμοποιείται ώστε να μεταφέρει μηνύματα λάθους και άλλες πληροφορίες σε unicast διευθύνσεις. Τα ICMP πακέτα ενθυλακώνονται μέσα σε IP datagrams.

Το Ping στέλνει ένα ή περισσότερα ICMP_ECHO πακέτα σε έναν host. Ο σκοπός μπορεί να είναι απλά να καθορίσει εαν ο host είναι "ζωντανός" (προσβάσιμος). Τα ICMP_ECHO πακέτα, μπορούν προαιρετικά να συμπεριλάβουν και ένα τμήμα δεδομένων (data section). Αυτά τα δεδομένα συνήθως αποτελούνται από πληροφορίες που αφορούν ένα συγκεκριμένο χρονικό σημείο, ώστε από το ICMP_ECHOREPLY μήνυμα που θα επιστραφεί, να εξαχθούν χρήσιμες πληροφορίες σχετικά π.χ με το χρόνο που χρειάζεται ένα πακέτο για έναν πλήρη κύκλο ταξιδιού. Έτσι τα trojan horses μπορούν να ενθυλακωθούν σε ένα ICMP_ECHO πακέτο, με αρνητικά αποτελέσματα.

Τα ICMP πακέτα είναι αρκετά επικίνδυνα για την ασφάλεια του δικτύου. Πολλοί administrators, ρυθμίζουν τα firewalls και τους δρομολογητές ούτως ώστε να μην επιτρέπουν τη διέλευση ICMP πακέτων, και να βασίζονται σε άλλα πρωτόκολλα, όπως το RIP ή το OPSF για την αναπλήρωση του διαχειριστικού κενού που αφήνει ο αποκλεισμός των Ping πακέτων.

1.3.1.3 Επίθεση με UDP πακέτα

Η επίθεση αυτή είναι γνωστή ως "Καταιγίδα UDP πακέτων" (UDP packet storm). Ένας μεγάλος αριθμός UDP πακέτων αποστέλλεται σε ένα σύστημα, με αποτέλεσμα την υποβάθμιση της απόδοσης του συστήματος που δέχεται τα πακέτα. Όταν εγκαθίσταται μια σύνδεση μεταξύ δυο UDP υπηρεσιών, κάθε μία από τις οποίες παράγει output, μπορεί να παραχθεί ένας πολύ υψηλός αριθμός UDP πακέτων, και από τις δυο υπηρεσίες. Εαν τα UDP πακέτα ανταλλάσσονται εκατέρωθεν, τότε η δυσλειτουργία παρουσιάζεται και στους δύο hosts.

1.3.2 Επιθέσεις Μεταμφίεσης (Spoofing)

Κατά τις επιθέσεις αυτές, ο επιτιθέμενος προσποιείται κάποιον άλλον, "μεταμφιέζεται" ώστε να αποκτήσει εξουσιοδοτημένη πρόσβαση στους πόρους ενός

συστήματος. Οι χαρακτηριστικότερες επιθέσεις του είδους είναι το IP Spoofing, το DNS Spoofing και το ARP spoofing.

1.3.2.1 IP Spoofing

Η επίθεση αυτή ουσιαστικά βασίζεται στις σχέσεις εμπιστοσύνης που υπάρχουν μεταξύ των δικτύων ή/και των συστημάτων κάθε δικτύου στο Internet. Γενικά, η επίθεση αυτή γίνεται από το root λογαριασμό του επιτιθέμενου host προς τον root λογαριασμό του host-θύματος.

Στη συνέχεια, θα χρησιμοποιήσουμε τους εξής συμβολισμούς:

A: Ο host-στόχος
B: Ο έμπιστος host (ο A εμπιστεύεται τον B)
X: Ο απροσέγγιστος host (δεν μπορεί να λάβει μηνύματα που απευθύνονται σε αυτόν)
Z: Ο επιτιθέμενος host.

Για να γίνει η επίθεση, ο επιτιθέμενος host Z πρέπει να ιδιοποιηθεί την ταυτότητα ενός έμπιστου host ως προς τον A. Στη συνέχεια απενεργοποιεί τον έμπιστο αυτόν host B, εξαπολύοντάς του μια TCP SYN επίθεση άρνησης υπηρεσίας. Κατόπιν αρχίζει ένα διάλογο με τον στόχο A, προσποιούμενος ότι είναι ο B. Ο host A, υπό κάποιες προϋποθέσεις που θα αναφέρουμε στη συνέχεια, νομίζει ότι μιλάει με τον "φίλο" του B.

Ο host Z στέλνει μεταμφιεσμένα (spoofed) IP datagrams στον A, τα οποία βρίσκουν το στόχο τους. Αυτό συμβαίνει, επειδή όπως έχουμε αναφέρει και νωρίτερα, το IP είναι connectionless πρωτόκολλο, επομένως κάθε datagram στέλνεται στον προορισμό του ανεξάρτητα από το αν έχει προϋπάρξει εγκατεστημένη σύνδεση μεταξύ δύο hosts. Τα datagrams που στέλνει πίσω ο A (τα οποία προορίζονται για τον έμπιστο host) δε φθάνουν ποτέ στο στόχο τους (αφού ο B έχει δεχθεί επίθεση). Αλλά ούτε ο Z μπορεί να τα δει. Οι ενδιάμεσοι δρομολογητές γνωρίζουν πού πρέπει να πάνε τα datagrams (στον host B). Όσον αφορά το επίπεδο Δικτύου, από εκεί προέρχονται, και εκεί πρέπει να κατευθυνθούν οι απαντήσεις. Φυσικά, όταν τα datagrams δρομολογηθούν εκεί (στον host B) και η πληροφορία αρχίσει να *αποπλέκεται* (demultiplexing) στο σωρό των πρωτοκόλλων, και φθάσει στο TCP, καταστρέφεται, εφόσον ο B δε μπορεί να απαντήσει.

Παρ'όλα αυτά, ο επιτιθέμενος πρέπει να *ξέρει* τί έστειλε ο A, αλλά πρέπει επίσης να ξέρει και ποιά απάντηση περιμένει ο server. Ο Z δεν μπορεί να δει αυτά που έστειλε ο A αλλά μπορεί να τα προβλέψει. Έτσι, μπορεί να συνεχίσει την επικοινωνία του με τον A.

Απαραίτητη προϋπόθεση για την επίθεση, είναι η γνώση ενός τουλάχιστον host που εμπιστεύεται ο host A. Εαν ο A δεν εμπιστεύεται κανέναν, τότε η επίθεση τελειώνει πριν αρχίσει. Στη συνέχεια, ο Z πρέπει να αποκτήσει μια ιδέα σχετικά με το "ποιός είναι ο 32-bit *αριθμος ακολουθίας* (sequence number) στα TCP segments που αποστέλλει ο A". Για να το κάνει αυτό, συνδέεται κανονικά (με την πραγματική του διεύθυνση) σε μια TCP port του A (π.χ SMTP) και πραγματοποιεί μαζί του ένα τριπλό handshake, αποθηκεύοντας τον ISN (Initial sequence Number) που χρησιμοποίησε ο A. Αυτή η διαδικασία επαναλαμβάνεται κάμποσες φορές και οι ISNs αποθηκεύονται ομοίως. Επίσης, ο Z υπολογίζει το μέσο *χρόνο κυκλικού ταξιδιού* (Round Trip Time, RTT) των πακέτων (από αυτόν στον A και πάλι σε αυτόν). Το RTT είναι απαραίτητο για την πρόβλεψη του επόμενου ISN.

Ως αυτή τη στιγμή, ο επιτιθέμενος έχει στη διάθεση του τα εξής στοιχεία: γνωρίζει τον τελευταίο ISN που χρησιμοποίησε ο A, ξέρει με τί ρυθμό αυξάνονται οι *αριθμοί ακολουθίας* και γνωρίζει πόσος περίπου χρόνος θα χρειαστεί ώστε ένα IP datagram να ταξιδέψει στο Internet για να φθάσει τον A.

Μέτρα πρόληψης

Η χρήση ενός καλά διαμορφωμένου δρομολογητή με δυνατότητες φιλτραρίσματος (packet filtering router) είναι επίσης απαραίτητη. Οι χρήστες του LAN δε θα πρέπει να αναπτύσσουν σχέσεις εμπιστοσύνης με κανέναν από τους hosts εκτός του LAN.

Επιπρόσθετα, το IP spoofing αποτρέπεται, εαν όλα τα πακέτα που εισέρχονται ή εξέρχονται του δικτύου κρυπτογραφούνται ή/και αυθεντικοποιούνται.

Τέλος, θα πρέπει να βρεθεί κάποιος μηχανισμός ώστε ο ISN να μη μπορεί να προβλεφθεί (να είναι τυχαίος και όχι ψευδο-τυχαίος).

1.3.2.2 DNS Spoofing

Όταν το software σε έναν host χρειάζεται να μετατρέψει ένα domain όνομα σε διεύθυνση, στέλνει ένα "ερώτημα εύρεσης διεύθυνσης" (address lookup query) σε έναν DNS server.'Οταν ένας client συνδέεται με έναν host που διαθέτει ένα domain όνομα, ο client πρέπει να μετατρέψει το όνομα σε IP διεύθυνση. Ο client εμπιστεύεται αφενός το DNS σύστημα ώστε να επιστρέψει τη σωστή διεύθυνση, αφετέρου το σύστημα δρομολόγησης ώστε να παραδώσει τα δεδομένα στον προορισμό τους. Το ίδιο συμβαίνει και όταν ο host χρειάζεται να μετατρέψει μια IP διεύθυνση σε domain όνομα. Τότε λέμε ότι απευθύνει ένα "ερώτημα εύρεσης ονόματος" (reverse lookup query).

Ένας DNS server ενδέχεται να έχει παραβιαστεί από κάποιον cracker. Όταν γίνει αίτηση σύνδεσης με τον server μας, ο server στέλνει αίτηση στον DNS server ώστε να μάθει ποιο domain name αντιστοιχεί στην αίτηση που ήλθε από μια δεδομένη IP address. Ο DNS server, εαν είναι παραβιασμένος, μπορεί να επιστρέψει το όνομα ενός "έμπιστου" domain και κατ' επέκταση "έμπιστου host".

Προκειμένου να ελαττωθεί ο κίνδυνος, ορισμένοι servers μπορούν να ρυθμιστούν ούτως ώστε να κάνουν έναν "έξτρα" έλεγχο για κάποιο client. Μετά δηλαδή από τον εντοπισμό (έπειτα από αίτηση στο DNS server) του host, ο server μας στέλνει άιτηση εύρεσης της IP διεύθυνσης που αντιστοιχεί στο host όνομα. Εαν οι δύο διεθύνσεις, η αρχική και η τελική, δε συμφωνούν, η αίτηση σύνδεσης με τον server απορρίπτεται. Οι πίνακες που περιέχουν ονόματα hosts για συγκεκριμένες IP διευθύνσεις, και οι πίνακες που περιέχουν IP διευθύνσεις για συγκεκριμένα ονόματα hosts, βρίσκονται συνήθως σε διαφορετικά αρχεία, και τα αρχεία αυτά βρίσκονται σε διαφορετικούς name servers. Έτσι, είναι σαφώς δυσκολότερο για έναν cracker να ελέγχει και τους δύο DNS servers.

1.3.2.3 ARP Spoofing

Το ARP (Address Resolution Protocol) αποτελεί αναπόσπαστο κομμάτι του Ethernet στο επίπεδο Πρόσβασης Δικτύου. Όταν ένα IP datagram είναι έτοιμο να παραδοθεί σε έναν host του Ethernet τοπικού δικτύου, ο host που έχει την ευθύνη να το παραδώσει, πρέπει να ξέρει τη hardware διεύθυνση προοορισμού που αντιστοιχεί στην IP διεύθυνση του datagram που διαθέτει. Για μη-τοπικές διευθύνσεις, η hardware διεύθυνση που θα χρησιμοποιήσει είναι η διεύθυνση ενός από τους δρομολογητές στο τοπικό δίκτυο.

Προκειμένου να βρει τη hardware διεύθυνση, ο host στέλνει μια "*αίτηση ARP*" με προορισμό την hardware broadcast διεύθυνση. Τα πακέτα με αυτήν τη διεύθυνση φθάνουν στα interfaces όλων των hosts του τοπικού δικτύου, προκαλώντας ένα interrupt στη CPU τους για περαιτέρω επεξεργασία. Λογικά, μόνον ένας host με την αντίστοιχη IP διεύθυνση θα στείλει μια "*απάντηση ARP*", και οι υπόλοιποι hosts θα αγνοήσουν την προηγούμενη *αίτηση*.

Οι αντιστοιχίες μεταξύ hardware και IP διευθύνσεων, στους υπολογιστές του

τοπικού δικτύου, αποθηκεύονται σε μια ARP cache για κάθε host. Όταν το IP datagram είναι έτοιμο να φύγει από έναν host, ο host συμβουλεύεται την ARP cashe ώστε να βρει τη hardware διεύθυνση προορισμού. Έαν ο host βρει μια είσοδο (entry) για την IP διεύθυνση, τότε δε χρειάζεται να αποστείλει μια *"αίτηση ARP"*. Οι είσοδοι στην ARP cashe εκπνέουν μετά από αρκετά λεπτά.

Όταν δυο υπολογιστές στο τοπικό δίκτυο έχουν την ίδια IP διεύθυνση , τότε έχει γίνει κάποιο λάθος, ή πραγματοποιείται μια ARP Spoofing επίθεση. Εαν ο "νόμιμος" υπολογιστής είναι κλειστός, τότε ο "μεταμφιεσμένος" υπολογιστής θα απαντάει σε *ARP αιτήσεις*, δίνοντας τη δική του hardware διεύθυνση. Έτσι, όλα τα IP πακέτα που προορίζονταν για το "νόμιμο" υπολογιστή, θα καταλήγουν στο μεταμφιεσμένο.

Όταν και οι δύο μηχανές (με την ίδια IP διεύθυνση) είναι εν ενεργεία, τότε θα απαντούν και οι δύο σε *ARP αιτήσεις*. Ο host που απήυθυνε την *"αίτηση"*, λογικά θα βρεθεί αντιμέτωπος με δυο απαντήσεις για μια συγκεκριμένη IP διεύθυνση. Αυτές οι απαντήσεις λογικά θα φθάσουν με χρονική διαφορά κάποιων milliseconds. Ορισμένα λειτουργικά συστήματα δε θα εντοπίσουν καμια ανωμαλία στην όλη διαδικασία, και θα χρησιμοποιήσουν την απάντηση που έφθασε αργότερα για να ανανεώσουν την ARP cashe. Άλλα λειτουργικά συστήματα, θα αγνοήσουν απαντήσεις που σχετίζονται με IP διευθύνσεις για τις οποίες υπάρχει ήδη είσοδος στην ARP cashe.

Επομένως, ανάλογα με το μηχανισμό που υϊοθετείται για την αντιμετώπιση των "διπλών" απαντήσεων σε ARP αιτήσεις, ο spoofer που θέλει να είναι ο στόχος των IP datagrams για συγκεκριμένη IP διεύθυνση, θα πρέπει είτε να είναι ο πρώτος, είτε ο τελευταίος που θα απαντήσει στην ARP αίτηση.

Αποτρέποντας μια ARP spoofing επίθεση

Η παραβίαση μπορεί να αποβεί αρκετά χρήσιμη σε έναν cracker, ιδίως εαν ο host, του οποίου προσεταιρίστηκε την IP διεύθυνση, απολαμβάνει την εμπιστοσύνη άλλων hosts. Οι hosts που εμπιστεύονται άλλους hosts, δεν πρέπει να χρησιμοποιούν το ARP για να αποκτούν τη hardware διεύθυνση αυτών των hosts. Αντίθετα, οι hardware διευθύνσεις των "έμπιστων" hosts θα πρέπει να φορτώνονται ως μόνιμες είσοδοι στην ARP cashe. Αντίθετα με τις κανονικές εισόδους της cashe, οι μόνιμες είσοδοι δεν εκπνέουν μετά από λίγα λεπτά. Η αποστολή ενός datagram σε μια IP διεύθυνση που σχετίζεται με μια μόνιμη είσοδο της cashe, δε θα έχει ποτέ ως αποτέλεσμα την αποστολή μιας ARP αίτησης.

Η διατήρηση μόνιμων εισόδων στην cashe, έχει ως αποτέλεσμα την αποστολή datagrams προς μια μηχανή ακόμα και αν η μηχανή αυτή δε λειτουργεί, κάτι που δεν είναι επιθυμητό. Επίσης, οι ARP cashes μπορεί να είναι περιορισμένου μεγέθους, κάτι που περιορίζει τον αριθμό των εισόδων που μπορούν να τοποθετηθούν.

1.3.3 Επιθέσεις Παρακολούθησης (Sniffing)

Sniffing είναι η χρήση ενός interface δικτύου προκειμένου να ληφθούν δεδομένα, τα οποία δεν προορίζονται για τον υπολογιστή στον οποίο υφίσταται το interface. Μια ποικιλία τύπων μηχανών, πρέπει να εχουν αυτήν τη δυνατότητα. Για παράδειγμα μια γέφυρα (bridge) σε ένα token ring δίκτυο (δακτυλίου με κουπόνι), έχει δυο interfaces δικτύου και κανονικά λαμβάνει όλα τα δεδομένα που διέρχονται από το φυσικό μέσο στο ένα interface, και μεταδίδει ορισμένα από αυτά τα πακέτα, αλλά όχι όλα, στο άλλο interface. Μια άλλη συσκευή η οποία ενσωματώνει το sniffing στη λειτουργία της, είναι αυτή που συνήθως καλείται "network analyzer". Ο analyzer βοηθάει το διαχειριστή ενός δικτύου στη διάγνωση μιας ποικιλίας προβλημάτων, που μπορεί να μην είναι ορατά σε οποιονδήποτε host.

Οι συσκευές με δυνατότητες sniffing είναι χρήσιμες και απαραίτητες. Εντούτοις, η ύπαρξή τους σημαίνει ότι και ένα "κακόβουλο" άτομο θα μπορούσε να τις χρησιμοποιήσει ώστε να συλλαμβάνει την κίνηση σε ένα δίκτυο. Υπάρχουν ειδικά sniffing προγράμματα, ορισμένα από τα οποία είναι δωρεάν, τα οποία μπορούν να χρησιμοποιηθούν για την παρακολούθηση:

- **Passwords** (συνθηματικών)
- **Στοιχείων οικονομικών συναλλαγών** (π.χ κωδικοί πιστωτικών καρτών)
- **Εμπιστευτικών δεδομένων** (π.χ e-mail, εγγραφών βάσεων δεδομένων σε μια client-server επικοινωνία)
- **Πληροφορίες πρωτοκόλλων χαμηλού επιπεδου** (π.χ οι *αριθμοί ακολουθίας* - sequence numbers- σε μια TCP σύνδεση)

Υπάρχουν αρκετά προληπτικά μέτρα που μπορεί να λάβει κανείς ώστε να αποτρέψει μια επίθεση παρακολούθησης:

- **Σωστή διαμόρφωση του δικτύου**: Κάθε *τμήμα δικτύου* (network segment) πρέπει να αποτελείται από μηχανές που εμπιστεύονται η μία την άλλη.

- **Χρήση κρυπτογραφημένων passwords**: Τα συνθηματικά θα πρέπει να κρυπτογραφούνται, πριν χρησιμοποιηθούν για οποιονδήποτε λόγο. Βέβαια, ακόμα και με την κρυπτογράφηση, ένας sniffer μπορεί να αποκτήσει το κρυπτογραφημένο password, και να προσπαθήσει να το αποκρυπτογραφήσει με την άνεσή του. Μια λύση είναι η κρυπτογράφηση όχι μόνο του password, αλλά του password και της τρέχουσας ώρας. Εαν ο αποστολέας και ο παραλήπτης είναι καλά συγχρονισμένοι, τότε ο sniffer πρέπει να "ξαναπαίξει" (replay) το κρυπτογραφημένο password μέσα σε ένα πάρα πολύ μικρό χρονικό χρονικό διάστημα (που καλείται "tick"), κάτι πολύ δύσκολο.
- **Κρυπτογράφηση για ολόκληρη τη Σύνδεση/Σύνοδο** (βλέπε κεφάλαιο 2, "Κρυπτογραφία και Web").

1.3.4 Άλλα προβλήματα ασφαλείας

Εκτός από τις περιπτώσεις που αναφέραμε, και οι οποίες είναι οι πιο συνήθεις στα περιβάλλοντα των TCP/IP δικτύων, αξίζει να αναφερθούμε και σε ορισμένες άλλες παραβιάσεις:

Session Hijacking (Πειρατεία Συνόδου): Έχοντας αποκτήσει root πρόσβαση σε ένα σύστημα, ένας cracker μπορεί να χρησιμοποιήσει κάποιο εργαλείο ώστε να μεταβάλλει το UNIX kernel. Αυτή η τροποποίηση επιτρέπει στον επιτιθέμενο να χειριστεί εξ'ολοκλήρου ήδη υπάρχουσες συνδέσεις από οποιονδήποτε χρήστη στο σύστημα, κάνοντας ό,τι θα μπορούσε να κάνει και ο χρήστης. Με αυτόν τον τρόπο, ο cracker παρακάμπτει τους όποιους μηχανισμούς αυθεντικοποίησης υπάρχουν στο σύστημα, αφού "αναλαμβάνει" τη σύνδεση του χρήστη αφότου αυθεντικοποιηθεί (ο χρήστης). Επίσης, ο cracker μπορεί να αποκτήσει πρόσβαση σε απομακρυσμένα sites "αναλαμβάνοντας" τη σύνδεση αφότου ο χρήστης αυθεντικοποιηθεί στο απομακρυσμένο site.

Επιθέσεις "σπασίματος" συνθηματικών (password cracking): Σήμερα υπάρχουν διαθέσιμα πολλά προγράμματα για "σπάσιμο" των passwords, τα οποία συγκρίνουν το αρχείο των passwords ενός συστήματος με ένα λεξικό κρυπτογραφημένων passwords.

Στόχος των επιθέσεων είναι κυρίως τα "αδύναμα" passwords .

Εκμετάλλευση λαθών (bugs) σε servers προσβάσιμους από το κοινό: Για παράδειγμα, πολλοί mail servers έχουν τρύπες ασφαλείας, που μπορούν να εκμεταλλευθούν από οποιονδήποτε. Παρότι το SMTP είναι από τα πιο σημαντικά πρωτόκολλα, η πιο κοινή υλοποίησή του, το πρόγραμμα sendmail, δημιούργησε στο παρελθόν πολλά προβλήματα ασφαλείας, ενώ οι εκδόσεις του διαδέχονταν οι μία την άλλη.

Παράλληλα, η συνδεση με telnet παρουσιάζει προβλήματα σε πολλές περιπτώσεις. Το Telnet παρέχει πρόσβαση τερματικού σε έναν host υπολογιστή. Ο χρήστης αυθεντικοποιείται συνήθως πληκτρολογώντας ένα όνομα και ένα συνθηματικό. Και τα δύο αυτά στοιχεία μεταφέρονται σε "καθαρή μορφή" (clear text) μέσω του δικτύου, οπότε είναι ευάλωτα. Στις telnet συνόδους (sessions) είναι απαραίτητος ένας ισχυρός μηχανισμός αυθεντικοποίησης, όπως επίσης και μηχανισμοί κρυπτογράφησης των δεδομένων που ανταλλάσσονται κατά τη διάρκεια της σύνδεσης.
Επίσης, οι επιθέσεις σε Web sites αυξάνονται συνεχώς, καθώς η HTML επιτρέπει και σε άλλα πρωτόκολλα εκτός του HTTP να χρησιμοποιηθούν (FTP,TELNET, RLOGIN, κ.α). Έτσι, η HTML μπορεί να χρησιμοποιηθεί ώστε να παρακαμφθούν τα φίλτρα που εφαρμόζονται σε αυτά τα πρωτόκολλα από τα firewalls. Άλλα προβλήματα περιλαμβάνουν: ασφάλεια των cgi scripts, ασφάλεια των Java applets, αμοιβαία αυθεντικοποίηση client/server σε οικονομικές συναλλαγές και εμπιστευτικότητα και ακεραιότητα των δεδομένων που ανταλλάσσονται.

1.4 Ασφαλίζοντας ένα TCP/IP δίκτυο

Πολλές επιχειρίσεις σήμερα βασίζονται σε δίκτυα υπολογιστών προκειμένου να προάγουν τα συμφέροντά τους. Πολύτιμα δεδομένα όπως και λειτουργίες ή διαδικασίες μεταφέρονται και εκτελούνται μέσω TCP/IP δικτύων, ή είναι προσβάσιμα μέσα σε αυτά. Οι εταιρίες πιέζονται συνεχώς προκειμένου να διευρύνουν τα δίκτυά τους ώστε οι εργαζόμενοι σε αυτές να δουλεύουν από το σπίτι τους, ή από laptop υπολογιστές.

Πολιτική

Το πρώτο βήμα που πρέπει να πράξει μια επιχείριση είναι ο καθορισμός μιας συγκεκριμένης πολιτικής ασφαλείας. Η πολιτική αυτή θα εκφράζεται με ένα σύνολο κανόνων, που θα καθορίζουν ένα σύνολο λειτουργιών και δικαιωμάτων ενός συνόλου αντικειμένων μέσα στο δίκτυο. Τα αντικείμενα αυτά μπορεί να είναι άνθρωποι, συστήματα υπολογιστών ή στοιχεία των συστημάτων.

Λειτουργίες ασφαλείας

Κάθε σύστημα ασφαλείας πρέπει να πληρεί δύο βασικές λειτουργίες: πρόληψη των επιθέσεων, ελέγχοντας τους χρήστες και προστατεύοντας τα δεδομένα, και ανίχνευση των επιθέσεων που έχουν ήδη πραγματοποιηθεί. Ανάμεσα στα μέτρα που μπορούν να ληφθούν, για την πρόληψη των επιθέσεων, είναι και τα ακόλουθα:

- **Αυθεντικοποίηση,** χρησιμοποιώντας ψηφιακές υπογραφές και πιστοποιητικά (certificates), ώστε υπάρχει σιγουριά ότι οι εν δυνάμει χρήστες είναι αυτοί που ισχυρίζονται ότι είναι.
- **Έλεγχος Πρόσβασης**, χρησιμοποιώντας passwords και Λίστες Ελέγχου Πρόσβασης (Access Control Lists) ή έξυπνες κάρτες (smart cads) και PINs (Personnal Identification Number) ώστε να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση σε μια υπηρεσία ή δεδομένα.
- **Εμπιστευτικότητα**, χρησιμοποιώντας κρυπτογράφηση δεδομένων, ώστε να

αποτρέπεται η μη εξουσιοδοτημένη αποκάλυψη πληροφοριών.

- **Έλεγχοι ακεραιότητας,** χρησιμοποιώντας κρυπτογράφηση και ψηφιακές υπογραφές, ώστε να ανιχνεύεται η μη εξουσιοδοτημένη δημιουργία, παραλλαγή ή σβήσιμο δεδομένων.
- **Καταλογισμός ευθύνης**, με τη χρήση ψηφιακών υπογραφών και πιστοποίησης από τρίτο μέρος, ώστε το συμβαλλόμενο μέρος σε μια συναλλαγή να μη μπορεί να αρνηθεί τις ενέργειές του.

Ανάμεσα στα μέτρα που μπορούν να ληφθούν, για την ανίχνευση των επιθέσεων, είναι και τα ακόλουθα:

- **Εργαλεία ελέγχου ορθότητας** (audit tools), όπως αρχεία log, ώστε να είναι γνωστό τί συνέβει στο παρελθόν.
- **Έλεγχοι σε πραγματικό χρόνο** (real-time monitoring), ώστε οι διαχειριστές των συστημάτων να ενημερώνονται αμέσως μόλις συμβεί μια παραβίαση ασφαλείας.

Μηχανισμοί και διαδικασίες

Οι λειτουργίες που μόλις περιγράψαμε ενισχύονται από μια ποικιλία μηχανισμών, ο πιο σημαντικός από τους οποίους είναι η κρυπτογράφηση. Ο κύριος σκοπός της κρυπτογραφίας είναι η ενίσχυση της εμπιστευτικότητας. Εντούτοις, η κρυπτογραφία μπορεί επίσης να χρησιμοποιηθεί και για την αυθεντικοποίηση, την ακεραιότητα και τον καταλογισμό ευθύνης. Άλλοι σημαντικοί μηχανισμοί που βασίζονται στην κρυπτογραφία, είναι: ψηφιακές υπογραφές, πιστοποιητικά δημόσιου κλειδιού, διαχείριση κλειδιών και πιστοποιητικών.

Οι μηχανισμοί, με τη σειρά τους, "χτίζονται" από ένα σύνολο διαδικασιών. Οι πιο σημαντικές από αυτές είναι τα *πρωτόκολλα* και οι *αλγόριθμοι*. Ένα πρωτόκολλο είναι μια σειρά από βήματα που πρέπει να ακολουθηθούν από δύο ή περισσότερα αντικείμενα, και έχει σχεδιαστεί για να πραγματοποιεί μια συγκεκριμένη εργασία. Πρωτόκολλα όπως το SET για τις πληρωμές και το S/MIME για το email, έχουν σχεδιαστεί ώστε να ασφαλίζουν συγκεκριμένες Internet εφαρμογές. Οι αλγόριθμοι -όπως ο DES ή ο RSA- είναι μαθηματικές διαδικασίες για την επίλυση προβλημάτων.

Προϊόντα

Τα προϊόντα που παρέχουν ασφάλεια, ανήκουν σε τέσσερις κύριες κατηγορίες:

- Αυθεντικοποίηση και έλεγχος πρόσβασης (π.χ έξυπνες κάρτες, kerberos)
- Εμπιστευτικότητα και ακεραιότητα (π.χ firewalls, Virtual Private Networks)
- audit και monitoring (π.χ anti-virus scanners)
- υπηρεσίες εμπιστοσύνης (π.χ κρυπτογραφικά toolkits)

Οι πρώτες τρεις κατηγορίες υποστηρίζουν τις λειτουργίες στις οποίες αναφερθήκαμε προηγουμένως. Η ολοένα και ανεπτυσσόμενη κατηγορία των υπηρεσιών εμπιστοσύνης (trust services), είναι περισσότερο πολύπλοκη. Περιλαμβάνει offline υπηρεσίες, toolkits, και προϊόντα διαχείρισης εμπιστοσύνης (trust management products). Τα τελευταία συνίστανται σε προϊόντα διαχείρισης κλειδιού, προϊόντα αρχών πιστοποιητικού (certificate authority) και ανάκτησης κλειδιού (key recovery). Οι υπηρεσίες εμπιστοσύνης, θα αρχίσουν με τον καιρό να υποστηρίζουν προϊόντα από τις τρεις πρώτες κατηγορίες.

Τα firewalls και οι anti-virus scanners είναι εδώ και καιρό στο προσκήνιο. Εντούτοις τα περισσότερα από τα προϊόντα που υπόσχονται ασφάλεια στο Internet είναι

καινούρια και δεν έχουν υποστεί διεξοδικό έλεγχο.

Προκειμένου να εγκαταστήσουν ένα ασφαλές περιβάλλον για τις Internet εφαρμογές τους, οι χρήστες θα πρέπει να χρησιμοποιήσουν προϊόντα από τις περισσότερες κατηγορίες. Δυστυχώς δεν υπάρχουν ακόμα standards για την αλληλο-συμβατότητα (interoperability) των προϊόντων.

1.4.1 Πολιτική ασφαλείας

Μία από τις σημαντικότερες διαδικασίες εξασφάλισης ασφάλειας σε ένα TCP/IP δίκτυο συνδεδεμένο στο Internet, και ίσως η λιγότερο ευχάριστη διαδικασία, είναι η κατάστρωση της πολιτικής ασφαλείας του δικτύου.Οι περισσότεροι αναζητούν μια *τεχνική* λύση στο πρόβλημα της ασφάλειας, ενώ λίγοι είναι αυτοί που αποφασίζουν να γράψουν σε ένα χαρτί τί πρέπει να γίνει προκειμένου να υπάρχει ασφάλεια σε ένα δίκτυο. Στις μέρες μας όμως, αυτό είναι πολύ σημαντικό.

Προσεγγίζοντας την απειλή

Το πρώτο βήμα προς την κατάστρωση της κατάλληλης πολιτικής, είναι η προσέγγιση, δηλαδή η γνώση των πιθανών απειλών κατά της ασφάλειας του δικτύου. Υπάρχουν τρεις συγκεκριμένες απειλές:

1) *Μη εξουσιοδοτημένη πρόσβαση:* "Είσοδος στο σύστημα από μη εξουσιοδοτημένο πρόσωπο.
2) *Ανεπιθύμητη αποκάλυψη πληροφορίας:* Οποιοδήποτε πρόβλημα που προκαλεί την φανέρωση πολύτιμης ή ευαίσθητης πληροφορίας σε άτομα που δε θα έπρεπε να έχουν πρόσβαση σε αυτή την πληροφορία.
3) *Άρνηση υπηρεσίας:* Οποιοδήποτε πρόβλημα που καθιστά δύσκολη ή αδύνατη την επιτέλεση παραγωγικής εργασίας από την πλευρά του συστήματος.

Η πρόσβαση σε αυτές τις απειλές, άρα και η διαδικασία αντιμετώπισής τους, πρέπει να γίνει σε συνάρτηση με το "πόσοι χρήστες ενδέχεται να επηρρεαστούν από μια απειλή" και το "πόσο ευαίσθητη είναι η πληροφορία που απειλείται". Για ορισμένες εταιρίες, *οι μη εξουσιοδοτημένες προσβάσεις* ενδέχεται να μειώνουν την εμπιστοσύνη που άλλες επιχειρήσεις δείχνουν προς αυτές. Αλλά για τις περισσότερες επιχειρήσεις, η μη εξουσιοδοτημένη πρόσβαση δεν αποτελεί σημαντική απειλή, εκτός και αν σε αυτήν την απειλή ενέχονται και οι άλλες δύο: η *ανεπιθύμητη αποκάλυψη πληροφορίας* και η *άρνηση υπηρεσίας*.

Κατανέμοντας τις ευθύνες

Μία προσέγγιση στην ασφάλεια ενός δικτύου είναι η κατανομή ευθυνών και ελέγχου σε μικρές ομάδες ατόμων μέσα στην επιχείρηση. Ας μην παραβλέπουμε ότι οι περισσότερες "επιθέσεις" λαμβάνουν χώρα σε συγκεκριμένα υπολογιστικά συστήματα, οπότε, κατανέμοντας τις υπευθυνότητες σε groups ατόμων, για συγκεκριμένα τμήματα του δικτύου, είναι μια αρκετά καλή πολιτική.

Τα subnets (υποδίκτυα) είναι ένα ισχυρό εργαλείο στην κατανομή ευθυνών. Ο διαχειριστής (administrator) ενός subnet γίνεται υπεύθυνος για την ασφάλεια του subnet και έχει την ευθύνη παροχής IP διευθύνσεων σε κάθε σύστημα που συνδέεται στο δίκτυο. Παρέχοντας IP διευθύνσεις σημαίνει πως ο administrator ελέγχει κατά κάποιον τρόπο ποιός συνδέεται στο δίκτυο. Επίσης γνωρίζει πολύ καλά ποιό host έχει μια IP διεύθυνση, και ποιός είναι υπεύθυνος για αυτό το host. Όταν ο subnet administrator δίνει μια IP διεύθυνση σε ένα σύστημα, ταυτόχρονα εξουσιοδοτεί τον διαχειριστή του συστήματος (system administrator) με συγκεκριμένες υπευθυνότητες σχετικά με την ασφάλεια του συστήματος. Παρόμοια, όταν ο system administrator παρέχει σε ένα χρήστη λογαριασμό σε ένα σύστημα, τότε και ο χρήστης με τη σειρά του έχει συγκεκριμένες ευθύνες.

Οι ευθύνες λοιπόν σε ένα δίκτυο διαμοιράζονται μεταξύ του διαχειριστή του δικτύου, διαχειριστή του subnet, του συστήματος, και τέλος του χρήστη. Σε κάθε σημείο αυτής της ιεραρχίας τα άτομα αναλαμβάνουν συγκεκριμένες αρμοδιότητες. Είναι συγκεκριμένο βέβαια για κάποιον, σε όποιο σημείο της ιεραρχίας βρίσκεται, να ξέρει τί ακριβώς πρέπει να κάνει και πώς να το κάνει.

Μία σημαντική πρωτοβουλία προς την κατεύθυνση του κατανεμημένου ελέγχου ασφάλειας ενός δικτύου που είναι συνδεδεμένο στο Internet είναι η δημιουργία ταχυδρομικών λιστών (mailing lists) σε κάθε διαχειριστικό επίπεδο. Ο διαχειριστής του συστήματος λαμβάνει πληροφορίες σχετικά με την ασφάλεια ενός δικτύου, τις "φιλτράρει" απαλλάσσοντας τις από περιττές για τα κατώτερα επίπεδα πληροφορίες και τις ανακατεύθυνει στον διαχειριστή του subnet. Αυτός, με τη σειρά του, τις ανακατευθύνει στους διαχειριστές των συστημάτων κατά τον ίδιο τρόπο, οι οποίοι εκτελούν ακριβώς την ίδια διαδικασία για του απλούς χρήστες. Σήμερα με την ύπαρξη των Intranets και την εξάπλωσή τους, η δημιουργία και διατήρηση ταχυδρομικών λιστών μέσα στα πλαίσια του δικτύου σε μια εταιρία, είναι μια εύκολη αλλά ταυτόχρονα πολύ αποτελεσματική διαδικασία.

Ο network administrator μπορεί να αναζητήσει πληροφορίες σχετικές με ασφάλεια, από διαφορετικές πηγές μέσα στο Internet.

Γράφοντας την πολιτική ασφάλειας

Η ασφάλεια ενός TCP/IP δικτύου που είναι συνδεδεμένο στο Internet είναι ανέφικτη αν ο καθένας μέσα στο δίκτυο δεν γνωρίζει τις ευθύνες του, όπως αναφέρθηκε παραπάνω. Είναι σημαντικό πάντως η πολιτική ασφαλείας να έχει γραφεί επάνω σε χαρτί, να υπάρχουν δηλαδή σε γραπτό κείμενο οι κανόνες που πρέπει να ακολουθούνται ώστε το δίκτυο να είναι ασφαλές. Έτσι, θα πρέπει να καθορίζονται:

- *Οι ευθύνες ενός απλού χρήστη του δικτύου*

Η πολιτική μπορεί να απαιτεί οι χρήστες να αλλάζουν τα password (συνθηματικά) τους ανά τακτά χρονικά διαστήματα, να χρησιμοποιούν passwords που υπακούουν σε κάποιους κανόνες , ή να πραγματοποιούν συχνούς έλεγχους προκειμένου να διαπιστώσουν εαν οι λογαριασμοί τους έχουν παραβιαστεί από κάποιον άλλον. Οτιδήποτε είναι αναμενόμενο από τους απλούς χρήστες, πρέπει να οριστεί ρητώς.

- *Οι ευθύνες του system administrator*

Η πολιτική μπορεί να απαιτεί την λήψη συγκεκριμένων μέτρων και την πραγματοποίηση διαδικασιών ελέγχου σε κάθε host από τον διαχειριστή του συστήματος. Επίσης, μπορεί να αναφέρεται σε συγκεκριμένες εφαρμογές οι οποίες δεν πρέπει να "τρέχουν" στους hosts οι οποίοι είναι συνδεδεμένοι στο δίκτυο.

- *Η σωστή χρήση των πόρων του δικτύου*

Πρέπει να γίνει σαφές ποιός μπορεί να κάνει χρήση των πόρων του δικτύου, τί πρέπει να κάνουν και τί δεν πρέπει να κάνουν. Εάν π.χ ένας οργανισμός παίρνει θέση ότι τα e-mails, τα αρχεία και το ιστορικό των δραστηριοτήτων κάθε συστήματος υπόκεινται σε έλεγχο ασφάλειας, πρέπει να γίνει σαφές στους χρήστες ότι αυτό λέει η πολιτική ασφάλειας.

- *Τί θα γίνει όταν υπάρξει κάποιο πρόβλημα στην ασφάλεια του δικτύου*

Τί πρέπει να γίνει όταν ανακαλυφθεί κάποιο πρόβλημα στην ασφάλεια του δικτύου; Ποιός πρέπει να ενημερωθεί; Πρέπει στην πολιτική να αναφέρονται ξεκάθαρα όλα τα βήματα που πρέπει να γίνουν μετά από μια "επίθεση", τί πρέπει να κάνουν οι διαχειριστές των συστημάτων, ή οι απλοί χρήστες.

1.4.2 Μηχανισμοί Αυθεντικοποίησης (Authentication Mechanisms)

Με τον όρο αυθεντικοποίηση, αναφερόμαστε στη διαδικασία εκείνη που αποδεικνύει ότι η ισχυριζόμενη ταυτότητα ενός χρήστη που προσπαθεί να συνδεθεί στο δίκτυο, είναι και η πραγματική εξουσιοδοτημένη ταυτότητα. Συστήματα αυθεντικοποίησης μπορεί να είναι hardware, software ή άλλοι μηχανισμοί οι οποίοι επιτρέπουν υπό προϋποθέσεις την πρόσβαση ενός χρήστη στους πόρους του υπολογιστικού συστήματος. Στο πιο απλό επίπεδο, ο διαχειριστής συστήματος που προσθέτει ένα νέο λογαριασμό χρήστη στο σύστημα, αποτελεί τμήμα του μηχανισμού αυθεντικοποίησης του συστήματος.

1.4.2.1 Passwords (συνθηματικά)

Τυπικά, ένας χρήστης αυθεντικοποιείται στο σύστημα πληκτρολογώντας το όνομα (UserID) και το συνθηματικό (Password) του, ως απάντηση σε μια προτροπή που του γίνεται από το σύστημα.

Τα "καλά" συνθηματικά είναι το πιο απλό αλλά σημαντικότερο κομμάτι στην ασφάλεια ενός δικτύου που είναι συνδεδεμένο στο Internet, αλλά και γενικότερα σε ένα δίκτυο. Περισσότερο από 80% των προβλημάτων ασφαλείας στο Internet θα είχαν αποφευχθεί, εαν είχαν επιλεγεί καλά passwords.

Υπάρχουν κάποιοι άτυποι κανόνες στην επιλογή ενός συνθηματικού. Αυτοί είναι οι ακόλουθοι:

1) Μην επιλέγετε το login σας ως pasword.
2) Μην χρησιμοποιείτε το όνομα ενός ανθρώπου ή ενός πράγματος.
3) Μην χρησιμοποιείτε ως password πρωσοπικές πληροφορίες όπως αρχικά ονόματος, αριθμός τηλεφώνου, όνομα δουλειάς, οργανωτική μονάδα κ.λ.π.
4) Μην πληκτρολογείτε συνεχόμενα γράμματα από το πληκτρολόγιο, π.χ qwerty.
5) Μην πληκτρολογείτε μια οποιαδήποτε λέξη ανάποδα, ή κάποιο όνομα.
6) Μην χρησιμοποιείτε μια ακολουθία αριθμών.
7) Μην χρησιμοποιείτε κάποιο password, που έχετε δει σε κάποιο βιβλίο που μιλάει για ασφάλεια στα δίκτυα, όσο καλό κι αν είναι αυτό το password.
8) Χρησιμοποιείστε ως password ένα συνονθύλευμα αριθμών και γραμμάτων.
9) Χρησιμοποιείστε το λιγότερο 6 χαρακτήρες.
10) Χρησιμοποιείστε μια φαινομενικά τυχαία επιλογή αριθμών κι γραμμάτων. (π.χ τα πρώτα γράμματα από κάποιες λέξεις μαζί με κάποιες ημερομηνίες κ.λ.π)

Είναι σημαντικό για ένα διαχειριστή συστήματος να μπορεί να εξασφαλίσει ότι οι χρήστες των hosts γνωρίζουν αυτούς τους κανόνες και τους υπακούουν στο έπακρον.

Χρονολογώντας το password (password aging)

Ένας μηχανισμός χρονολόγησης των passwords που επιλέγονται από το χρήστη συνίσταται στην πρόβλεψη ενός ανώτατου χρονικού ορίου, μέσα στα πλαίσια του οποίου θα επιτρέπεται σε κάποιον χρήστη να χρησιμοποιεί το ίδιο password. Κατ' αυτόν τον τρόπο, όλα τα passwords έχουν συγκεκριμένο χρόνο ζωής, μετά το πέρας του οποίου ο χρήστης ειδοποιείται πως πρέπει να αλλάξει το password του. Εάν το password δεν αλλάξει μέσα σε σύντομο χρονικό διάστημα, τότε ο χρήστης χάνει το δικαίωμα χρησης του λογαριασμού του.

1.4.2.2 One-time Passwords (Συνθηματικά Μιας-Χρήσης)

Σήμερα, χρησιμοποιούνται ολοένα και περισσότερο one-time password συστήματα, όπως το S/KEY ή το SecurID της Security Dynamics Inc. Αυτά τα συστήματα, απαιτούν από τους χρήστες ένα καινούριο password κάθε φορά που συνδέονται στο σύστημα.

1.4.2.3 Challenge/Response μηχανισμοί

Μια άλλη προσέγγιση στο μηχανισμό αυθεντικοποίησης με συνθηματικά, είναι ένας μηχανισμός **ερωτο-απαντήσεων,** που εκτός από το συνθηματικό, ζητάει από το χρήστη και κάποιες άλλες πληροφορίες οι οποίες είναι γνωστές τόσο στο χρήστη, όσο και στο σύστημα όπου ο χρήστης προσπαθεί να συνδεθεί .

1.4.2.4 Έξυπνες κάρτες (Smart Cards)

Ορισμένα συστήματα χρησιμοποιούν τα λεγόμενα Smart Cards (έξυπνες κάρτες), μια συσκευή που μοιάζει με ένα computer τσέπης, ώστε να αυθεντικοποιούν χρήστες .Τα συστήματα αυτά, βασίζονται στην κατοχή, από την πλευρά του χρήστη, ενός αντικειμένου. Ένα τέτοιο σύστημα, για παράδειγμα, χρησιμοποιεί ένα μηχανισμό password, ζητώντας από το χρήστη να πληκτρολογήσει μια λέξη, την οποία ο χρήστης θα δει στο Smart Card του. Δηλαδή, ο host θα δώσει στο χρήστη κάποιου είδους πληροφορία, την οποία ο χρήστης θα πληκτρολογήσει στο πληκτρολόγιο του Smart Card του, και το Smart Card θα δώσει μια απάντηση στο χρήστη, η οποία θα πρέπει να πληκτρολογηθεί στο πληκτρολόγιο του host, πρωτού επιτευχθεί η πλήρης σύνδεση.

Υπάρχουν και άλλα συστήματα αυθεντικοποίησης όπως ανιχνευτές δακτυλικών αποτυπωμάτων**,** που όμως είναι πολυδάπανες επιλογές για την ασφάλεια ενός δικτύου, τουλάχιστον την παρούσα στιγμή.

1.4.2.5 Kerberos

Το Kerberos, που πήρε το όνομά του από το σκύλο-φύλακα των πυλών του Άδη, είναι μια συλλογή από software που χρησιμοποιείται σε ένα ευρύ δίκτυο προκειμένου να αυθεντικοποιήσει ένα χρήστη που επιχειρεί να συνδεθεί στο δίκτυο. Αναπτύχθηκε στο Massachussetts Institute of Technology (MIT). Χρησιμοποιεί ένα συνδυασμό *κρυπτογράφησης* και *κατανεμημένων βάσεων δεδομένων* ώστε ο χρήστης, εφόσον αποδείξει την ταυτότητά του, να μπορεί να συνδεθεί στο δίκτυο από οποιοδήποτε σταθμό εργασίας αυτός επιθυμεί. Παρ'ότι το Kerberos αποτελεί ένα αρκετά μεγάλο βήμα στον τομέα της αυθεντικοποίησης, υπάρχουν κάποιες αδυναμίες στο πρωτόκολλο που δημιουργούν προβλήματα ασφαλείας.

1.4.3 Μηχανισμοί Ακεραιότητας (Integrity Mechanisms)

Η ακεραιότητα της πληροφορίας αναφέρεται στην κατάσταση εκείνη της πληροφορίας κατά την οποία παραμένει πλήρης, σωστή και απαράλλαχτη από την τελευταία φορά που είχε πιστοποιηθεί η ακεραιότητά της. Η αξία της ακεραιότητας πληροφορίας, ποικίλλει ανάλογα με το site. Για παράδειγμα, για κυβερνητικές ή στρατιωτικές εγκαταστάσεις, είναι πολύ πιο σημαντική προτεραιότητα από ότι για άλλες επιχειρήσεις.

Υπάρουν αρκετοί μηχανισμοί, όπως και διαδικαστικοί έλεγχοι, οι οποίοι φροντίζουν για την ακεραιότητα της πληροφορίας.

Checksums

Ο απλούστερος μηχανισμός, μια ρουτίνα checksum, μπορεί να υπολογίσει μια

αριθμητική τιμή από ένα αρχείο συστήματος (το μέγεθος δηλαδή του αρχείου) και να τη συγκρίνει με την αμέσως προηγούμενη έγκυρη τιμή που γνώριζε. Εαν οι δύο αυτές τιμές είναι ίδιες, τότε το αρχείο είναι πιθανότατα απαράλλαχτο.

Ένας αποφασισμένος hacker μπορεί να παρακάμψει το μηχανισμό αυτό, προσθέτοντας ή αφαιρώντας χαρακτήρες από ένα αρχείο ώστε να φαίνεται ότι δεν έχει τροποποιηθεί.

Ένας ειδικός τύπος checksum, που καλείται CRC checksum, είναι περισσότερο "αυστηρός" και αποτελεσματικός από την απλή ρουτίνα checksum που περιγράψαμε προηγουμένως, αλλά είναι δύσκολο να τεθεί σε εφαρμογή.

Τα checksums δεν προστατεύουν την ακεραιότητα των δεδομένων, απλά "πληροφορούν" εαν αυτή έχει παραβιαστεί. Για την προστασία της πληροφορίας καθ'αυτής, πρέπει να χρησιμοποιούνται άλλοι μηχανισμοί όπως έλεγχοι πρόσβασης ή κρυπτογραφία.

Κρυπτογραφικά Checksums

Το κρυπτογραφικό checksum, συνίσταται στη διάσπαση του αρχείου σε μικρότερα κομμάτια, τον υπολογισμό ενός CRC checksum για κάθε κομμάτι, και τέλος την πρόσθεση όλων των CRCs μαζί. Ανάλογα με τον αλγόριθμο που θα χρησιμοποιηθεί, αυτή η μέθοδος συνιστά μια αρκετά καλή προσέγγιση στην ανίχνευση τροποποίησης ενός αρχείου δεδομένων.

Αυτός ο μηχανισμός βέβαια, καταναλώνει πολλά resources από το σύστημα που τον μεταχειρίζεται για την εξασφάλιση της ακεραιότητας των δεδομένων. Έτσι, επίκειται στους διαχειριστές συστημάτων να αποφασίσουν εαν επιθυμούν να το χρησιμοποιήσουν.

1.4.4 Έλεγχοι Ασφαλείας (Security Monitoring)

Δεν νοείται ασφάλεια σε ένα TCP/IP δίκτυο, χωρίς την ύπαρξη των εργαλείων εκείνων, που δίνουν τη δυνατότητα στους διαχειριστές του δικτύου να γνωρίζουν τις αδυναμίες των συστημάτων, τις αιτίες παρελθόντων παραβιάσεων, αλλά και γενικά το τί συμβαίνει στα συστήματα του δικτύου σε μια δεδομένη στιγμή.

1.4.4.1 Ανίχνευση των συστημάτων για αδυναμίες

Μια τέτοια διαδικασία ανίχνευσης, θα πρέπει να γίνεται περιοδικά στα εσωτερικά συστήματα του δικτύου (π.χ μια φορά το μήνα). Η όλη διαδικασία πραγματοποιείται με την εκτέλεση του κατάλληλου προγράμματος από έναν συγκεκριμένο κεντρικό host. Εαν το software το επιτρέπει, η ανίχνευση είναι σκόπιμο να αφορά όχι συγκεκριμένα συστήματα, αλλά ένα εύρος συστημάτων στο εσωτερικό δίκτυο. Με αυτόν τον τρόπο, ανιχνεύονται και προσφάτως εγκατεστημένα συστήματα.

Εαν το software που χρησιμοποιείται υποστηρίζει περισσότερες από μια βάσεις δεδομένων για την αποθήκευση των αποτελεσμάτων του ελέγχου ασφαλείας, είναι προτιμότερη η δημιουργία ξεχωριστής βάσης δεδομένων για κάθε segment ή πλατφόρμα (OS). Επίσης, είναι σημαντικό το software να έχει τη δυνατότητα αποστολής αναφορών μέσω email, το οποίο θα αποστέλλεται σε συγκεκριμένη email διεύθυνση για τη διατήρηση αποτελεσμάτων ελέγχου ασφαλείας.

Υπάρχουν αρκετά προγράμματα, δωρεάν αλλά και εμπορικά, τα οποία ειδικεύονται σε ελέγχους συστημάτων για αδυναμίες και τρωτά σημεία. Στα δωρεάν πακέτα, συγκαταλέγονται και τα ακόλουθα:

- SATAN

- ISS (Internet Security Scanner)
- NetProbe (PD)
- NSS (Network Security Scanner)

SATAN

Το SATAN έκανε την εμφάνισή του στο Internet στις 5 Απριλίου του 1995 , και προκάλεσε μεγάλη αναστάτωση στην κοινότητα των χρηστών του Internet, ακριβώς επειδή ελέγχει την ασφάλεια των συστημάτων εφαρμόζοντας μεθόδους που χρησιμοποιούνται από crackers για την παραβίασή τους, ενώ ταυτόχρονα έχει διατεθεί στο ευρύ κοινό. Το πρόγραμμα έχει γραφτεί σε κώδικα C, αλλά και σε κώδικα Perl. Επίσης, περιέχει HTML έγγραφα για τη χρήση του. Θεωρητικά είναι γραμμένο για τους διαχειριστές των συστημάτων, αλλά πρακτικά οποιοσδήποτε χρήστης το κάνει compilation στο σύστημά του, και με κάποιες άλλες αλλαγές, μπορεί να το εκτελέσει.

Το SATAN ανακαλύπτει και αναφέρει ποικίλλα λάθη και αδυναμίες στις υπηρεσίες ενός δικτύου, παρατίθοντας χρήσιμες και λεπτομερείς πληροφορίες στα αποτελέσματα που εξάγει. Αποτελείται από μερικά υπο-προγράμματα, κάθε ένα από τα οποία είναι ένα εκτελέσιμο αρχείο που εξετάζει έναν host για πιθανές αδυναμίες. Ένα σημαντικό πλεονέκτημα είναι η custom πρόσθεση ενός ελέγχου, διαφορετικού από αυτούς που πραγματοποιεί το πρόγραμμα, τοποθετώντας απλά ένα εκτελέσιμο αρχείο με την κατάληξη ".sat" στο κυρίως directory: το driver πρόγραμμα θα το εκτελέσει αυτόματα. Ο driver δημιουργεί ένα σύνολο "στόχων" και έπειτα εκτελεί κάθε ένα από τα προγράμματα "εναντίον" του στόχου. Στη συνέχεια, ένα άλλο πρόγραμμα "φιλτράρει" και αναλύει το output, ενώ ένα άλλο πρόγραμμα προσδίδει στα τελικά αποτελέσματα μια πιο "ευανάγνωστη" μορφή.

1.4.4.2 Συστήματα γενικού ελέγχου ασφαλείας δικτύων

Υπάρχουν ορισμένα προγράμματα τα οποία εκτελούν συνεχείς real-time ελέγχους στο δίκτυο, ελέγχοντας για μη εξουσιοδοτημένη πρόσβαση, για αδυναμίες των συστημάτων, ή ακόμα και αποτρέποντας πιθανές παραβιάσεις. Έτσι, οι TCP Wrappers αλλά και το IP-Watcher ξεχωρίζουν ώς δυο από τα πιο απαραίτητα εργαλεία στα χέρια του administrator.

TCP Wrappers

Οι TCP_Wrappers καταγράφουν το όνομα & την IP διεύθυνση του μηχανήματος που ζήτησε τη σύνδεση όπως και να εκτελούν και κάποιους άλλους συμπληρωματικούς ελέγχους. Αμέσως μετά εκτελούν την ζητούμενη εφαρμογή του server και περιμένουν για νέα κλήση.

Το θετικό του όλου προγράμματος είναι ότι δεν συνδυαλέγεται με τον client και με τη διεργασία του, ούτε με τον server. Αυτό του δίνει τη δυνατότητα να μην εξαρτάται από την εφαρμογή, ώστε να μπορεί να προστατεύει πολλά είδη υπηρεσιών δικτύου καθώς και να μην είναι ορατός από μακριά.

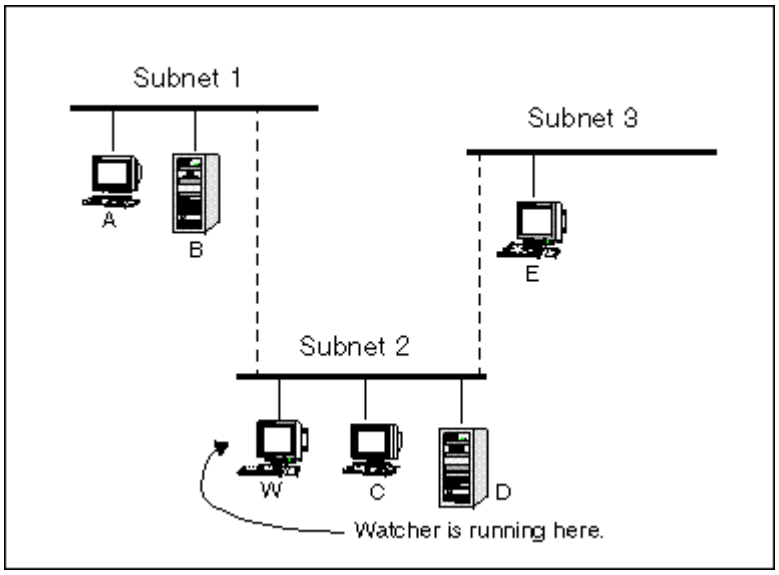
Ίσως ένα αρνητικό στοιχείο του προγράμματος είναι ότι, ακριβώς επειδή το πρόγραμμα απομακρύνεται αφού έχει πραγματοποιηθεί η σύνδεση, δεν μπορεί να ελέγξει δαίμονες (deamons) δικτύου που εξυπηρετούν περισσότερους από έναν clients. Θα μπορούσαν να δουν μόνο τον πρώτο από αυτούς που θα προσπαθούσε να συνδεθεί.

IP-Watcher

Το IP-Watcher είναι ένα διαχειριστικό εργαλείο για την ασφάλεια ενός δικτύου,

το οποίο δίνει τη δυνατότητα στον διαχειριστή να καταγράφει και να *ελέγχει* όλες τις login συνόδους στο δίκτυό του. Έτσι, ο διαχειριστής μπορεί εμφανίσει ένα ακριβές αντίγραφο της συνόδου σε πραγματικό χρόνο, όπως ακριβώς βλέπει τα δεδομένα και ο χρήστης. Το πρόγραμμα διαθέτει ένα απλό interface το οποίο επιδεικνύει όλες τις συνδέσεις που "βλέπει" καθώς και στατιστικά για το δίκτυο. Το IP-Watcher μπορεί να παρακολουθεί (monitor) όλες τις συνδέσεις οι οποίες υφίστανται στο subnet στο οποίο εκτελείται το IP-Watcher.

Με δεδομένη την τοπολογία στο σχήμα .6, το IP-Watcher μπορεί να παρακολουθεί συνδέσεις στα πλαίσια του subnet του (π.χ D με C), συνδέσεις από το εξωτερικό στο subnet του (π.χ A με C, E με D), όλες τις εξερχόμενες συνδέσεις (π.χ C με A, D με B) ή όλες τις συνδέσεις που διέρχονται από το subnet (π.χ E με A, B με E). Οι συνδέσεις που δεν μπορεί να "δει", είναι συνδέσεις που δε διέρχονται από το subnet όπου εκτελείται (π.χ A με B).



Σχήμα 6 Τοποθέτηση του IP Watcher

1.4.5 Περιορίζοντας την πρόσβαση στο δίκτυο

Τα κυρίαρχα πρωτόκολλα δικτύου που χρησιμοποιούνται στο Internet, όπως το IP, το TCP, το UDP, μπορούν να "κουβαλάνε" ορισμένες πληροφορίες ελέγχου οι οποίες μπορούν να χρησιμοποιηθούν ώστε να περιοριστεί η πρόσβαση σε κάποιους hosts ή δίκτυα μέσα σε μια επιχείρηση . Η επικεφαλίδα ενός IP packet περιέχει, όπως είδαμε,
τις διευθύνσεις δικτύου, τόσο του αποστολέα, όσο και του παραλήπτη του packet. Επιπλέον, τα πρωτόκολλα TCP και UDP εμπεριέχουν την έννοια της "θύρας" (port), η οποία προσδιορίζει το τελικό σημείο ενός μονοπατιού επικοινωνίας (συνήθως ένας Network server). Είναι εφικτό, σε κάποιες περιπτώσεις, να μη γίνεται δεκτή η πρόσβαση σε συγκεκριμένες TCP ή UDP θύρες, ή ακόμα και σε hosts ή δίκτυα.

Πίνακες Δρομολόγησης των Gateways (Gateway Routing Yables)

Μία από τις απλούστερες προσεγγίσεις στην αποφυγή ανεπιθύμητων συνδέσεων σε δίκτυο είναι η "αφαίρεση" ορισμένων δικτύων από τους πίνακες δρομολόγησης του gateway. Έτσι, είναι "αδύνατο" για έναν host να στείλει packets σε αυτά τα δίκτυα. Τα περισσότερα πρωτόκολλα απαιτούν αμφίδρομη ροή "πακέτων" ακόμα και για μια μονόδρομη αποστολή "πακέτων", οπότε αφαιρώντας κάποια δίκτυα από τον πίνακα

δρομολόγησης του gateway (ή αλλοιώς router) που συνδέει το δίκτυο μας με το Internet, δεν επιτρέπει στους hosts των δικτύων αυτών να συνδεθούν με το δικό μας δίκτυο.

Φιλτράρισμα Πακέτων από Routers (Router Packet Filtering)

Αρκετά gateway συστήματα (καλούμενα και δρομολογητές ή routers), έχουν την ικανότητα να "φιλτράρουν", δηλαδή να ελέγχουν πακέτα που διέρχονται από αυτά, βασισμένα όχι μόνο στη διεύθυνση δικτύου ή host του αποστολέα ή του παραλήπτη, αλλά σε ένα συνδυασμό διευθύνσεων αποστολέα και παραλήπτη. Αυτός ο μηχανισμός χρησιμοποιείται για να αποτραπεί η σύνδεση σε ένα συγκεκριμένο host, δίκτυο ή subnet, από οποιοδήποτε άλλο συγκεκριμένο host, δίκτυο ή subnet.

Υπάρχουν επίσης gateway συστήματα (π.χ Cisco Systems), που υποστηρίζουν ένα ακόμα πιο πολύπλοκο σχήμα, ασκώντας εκλεπτυσμένο έλεγχο στις διευθύνσεις αποστολέα και παραλήπτη, και απαγορεύοντας για παράδειγμα (με τη χρήση address masks) την πρόσβαση σε όλους εκτός από έναν host σε ένα συγκεκριμένο δίκτυο.

Firewalls

Αρκετές συζητήσεις γίνονται σήμερα σχετικά με τα συστήματα firewalls. Ο όρος firewall υποννοεί "προστασία από κίνδυνο". Έτσι, ένα firewall υπολογιστικό σύστημα προστατεύει ένα δίκτυο από τον εξωτερικό κόσμο. Περισσότερα για τα firewalls αλλά και για τους filtering δρομολογητές,στο κεφάλαιο 3.

Κρυπτογραφία και Web

2

2.1 Εμπόριο και Internet

Η ασφάλεια της πληροφορίας συνίσταται σε τρία πράγματα: εμπιστευτικότητα (confidentiality), ακεραιότητα, (integrity) και διαθεσιμότητα (availability) των δεδομένων. Η ασφάλεια του εμπορίου στο Web είναι ίσως η μεγαλύτερη πρόκληση που έχουν να αντιμετωπίσουν οι "ειδικοί" στο χώρο της ασφάλειας στο Web και το Internet γενικότερα.

Πριν μερικά χρόνια το εμπόριο στο Web δεν υπήρχε καν ως όρος. Σήμερα, προκαλεί το ενδιαφέρον οικονομικών κολοσσών. Επενδυτές συρρέουν στο χώρο και δημιουργούν εταιρίες που υπόσχονται την κατασκευή του απαραίτητου hardware και software που απαιτείται για τη διεκπεραίωση εμπορικών συναλλαγών. Εταιρίες επενδύουν μεγάλα χρηματικά ποσά στην αγορά του hardware και του software. Αλλά, τί είναι το "εμπόριο στο Internet";

Για μερικούς, εμπόριο στο Internet σημαίνει "λαμβάνω παραγγελίες με πιστωτική κάρτα, από πελάτες που ψωνίζουν επιλέγοντας προϊόντα από ηλεκτρονικούς καταλόγους στο Web". Για άλλους, εμπόριο στο Internet σημαίνει "η ηλεκτρονική συναλλαγή μεταξύ πελατών και προμηθευτών μέσω ενός ιδιωτικού δικτύου". Το ιδιωτικό αυτό δίκτυο καλείται συνήθως Εικονικό Ιδιωτικό Δίκτυο (Virtual Private Network) ή απλά VPN. Μία τρίτη τέλος υπόσταση του όρου είναι απλά η "ψηφιακή αυθεντικοποίηση", οποιουδήποτε τύπου δεδομένων στο Internet.

Τα θέματα που προέκυψαν από την εμφάνιση των συνθηκών για εμπόριο στο Web, επηρρεάζουν εκατοντάδες εταιριών, μικρών ή μεγάλων. Το Internet αποτελεί δέλεαρ κυρίως για μικρές εταιρίες, καθώς τους επιτρέπει να προσεγγίσουν ένα ευρύ αγοραστικό κοινό, με τρόπο όχι λιγότερο εντυπωσιακό από αυτόν που υϊοθετούν άλλες μεγαλύτερες εταιρίες.

Προβλήματα

Ένας διάχυτος φόβος αιωρείται στην κοινότητα των χρηστών του Web, πως εμπιστευτικά δεδομένα όπως αριθμοί πιστωτικών καρτών, μπορεί να αποκτηθούν από τρίτους κατά τη μετάδοσή τους στο Internet. Η πρόκληση που εμφανίζεται, είναι η λήψη και αποστολή πληροφοριών μέσω του Internet, παράλληλα με την εξασφάλιση ότι:

- Δεν υπάρχει πρόσβαση σε αυτές, από κανέναν εκτός του αποστολέα και του παραλήπτη (ιδιωτικότητα, **privacy**)
- Δεν μεταβάλλονται ή παραλλάσσονται κατά τη μεταφορά τους (ακεραιότητα, **integrity)**
- Ο παραλήπτης μπορεί να είναι σίγουρος ότι προέρχονται από τον αποστολέα (αυθεντικοποίηση, **authenticity**)
- Ο αποστολέας μπορεί να είναι σίγουρος ότι ο παραλήπτης είναι αυθεντικός (μη-μεταμφίεση, **non-fabrication**)
- Ο αποστολέας δεν μπορεί να αρνηθεί ότι τις απέστειλε (μη-καταλογισμός ευθύνης, **non-repudiation**)

Χωρίς ειδικά διατεθειμένο software, όλα τα δεδομένα "ταξιδεύουν" με στην αρχική τους μορφή, οπότε οποιοσδήποτε που έχει τα μέσα να παρακολουθεί την κίνηση των δεδομένων, μπορεί να τα αποκτήσει. Η επίθεση αυτή λέγεται packet sniffing, και είναι εύκολο να πραγματοποιηθεί σήμερα, όπου κυκλοφορεί δωρεάν μεγάλη ποσότητα κατάλληλου software. Το Internet θεωρούνταν πάντα ένα "ανοικτό" δίκτυο…

Η προστασία των συναλλαγών, αποτελεί τη μία πτυχή του προβλήματος. Άπαξ και η εμπιστευτική πληροφορία λαμβάνεται εκ μέρους του client, πρέπει να προστατευτεί στον server. Σήμερα, οι Web servers αποτελούν τον αγαπημένο στόχο των hackers. Αυτό ενισχύεται και από το γεγονός ότι σήμερα, πολλές Web εφαρμογές απαιτούν την αλληλεπίδραση του Web server με βάσεις δεδομένων των εταιριών, δημιουργώντας έτσι ένα σύνδεσμο (link) με τα εσωτερικά τοπικά δίκτυα. Η τεχνολογία των firewalls μπορεί να προσφέρει πολλά σε αυτόν τον τομέα, αρκεί να χρησιμοποιείται σωστά.

Το TCP/IP

Η εντυπωσιακή εξάπλωση και αποδοχή του Internet αποδεικνύει ότι το TCP/IP, πάνω στο οποίο είναι χτισμένο, έχει λύσει πολλά προβλήματα και έχει βοηθήσει σε πολλούς τομείς . Όμως, η αλήθεια είναι ότι το TCP/IP δεν σχεδιάστηκε για να προσφέρει ασφαλείς υπηρεσίες επικοινωνίας. Έτσι, εμφανίστηκε η ανάγκη της υϊοθέτησης καινούριων τεχνολογιών με σκοπό, εκτός από τη λύση των προβλημάτων που αναφέρθηκαν, και την την απάντηση των ακόλουθων ερωτημάτων:

- Πώς εξασφαλίζεται η παρόχη όλων των υπηρεσιών (Web, proxy, mail, news κ.λ.π) με ένα απλό login χρήστη, από ώστε να αποφεύγεται η διαχείριση από όλους τους servers των λογαριασμών χρηστών;
- Πώς εξασφαλίζεται ότι αυτές οι υπηρεσίες δουλεύουν όχι μόνο στο intranet αλλά και στο Internet; Με άλλα λόγια, πώς μπορεί να αποφευχθεί η διαχείριση διαφορετικών σχημάτων ασφαλείας εντός και εκτός του firewall;
- Πώς μπορεί να εξασφαλιστεί η ιδιωτικότητα (privacy) των επικοινωνιών, τόσο σε αυτές που εξελίσσονται σε πραγματικό χρόνο (όπως τα δεδομένα που ρέουν μεταξύ ενός Web client και ενός Web server), όσο και στις αποθήκευσε-και-προώθησε (store and forward) εφαρμογές όπως το e-mail;

Όλα τα προβλήματα και τα ερωτήματα που τέθησαν εως τώρα, μπορούν να λυθούν και να απαντηθούν αντίστοιχα, χρησιμοποιώντας την επιστήμη της κρυπτογραφίας. Σίγουρα πάντως τα προβλήματα δεν έχουν λυθεί, τουλάχιστον εντελώς, ως αυτήν τη στιγμή.

2.2 Κρυπτογραφία

Η κρυπτογραφία συνιστά μια οικογένεια τεχνολογιών που περιλαμβάνει τα ακόλουθα:

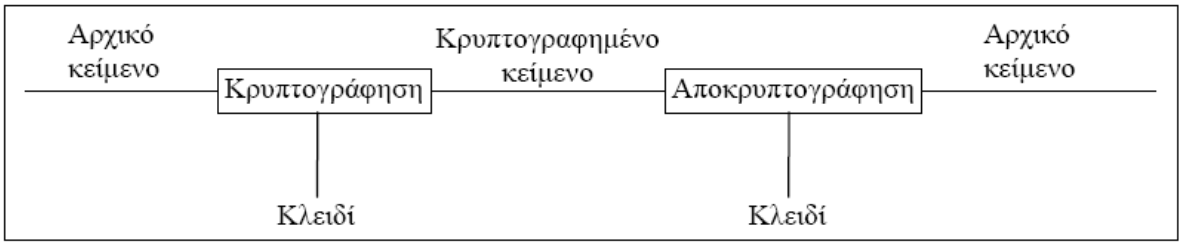
- Η Κρυπτογράφηση (**Encryption**) μετατρέπει τα δεδομένα σε μια μη αναγνώσιμη μορφή, ώστε να εξασφαλίσει την ιδιωτικότητα (privacy). Η επικοινωνία στο Internet μοιάζει με την αποστολή μιας ευχετήριας κάρτας στην καθημερινή ζωή. Η κρυπτογράφηση προσφέρει το ψηφιακό ισοδύναμο ενός σφραγισμένου φακέλου.
- Η Αποκρυπτογράφηση (**Decryption**) είναι το ακριβώς αντίθετο της κρυπτογράφησης. Μετατρέπει τα κρυπτογραφημένα δεδομένα στην αρχική ευανάγνωστη μορφή τους.
- Η ψηφιακή υπογραφή (**Digital signature**) "συνδέει" ένα document με τον κάτοχο μιας συγκεκριμένης πληροφορίας (που καλείται κλειδί ή key), και αποτελεί το ψηφιακό ισοδύναμο της υπογραφής επάνω σε χαρτί.

- Η πιστοποίηση της υπογραφής (**Signature Verification**) είναι το ακριβώς αντίθετο της ψηφιακής υπογραφής. Πιστοποιεί ότι μια συγκεκριμένη υπογραφή είναι αυθεντική.

Ένας κρυπτογραφικός αλγόριθμος, είναι η μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση . Η μοντέρνα κρυπτογραφία, χρησιμοποιεί ένα κλειδί (key), οποίο έχει ένα ευρύ σύνολο τιμών. Τόσο η κρυπτογράφηση, όσο και η αποκρυπτογράφηση, κάνουν χρήση αυτού του κλειδιού.

Αλγόριθμοι μυστικού κλειδιού

Ορισμένοι αλγόριθμοι είναι σχεδιασμένοι κατά τέτοιον τρόπο ώστε το κλειδί κρυπτογράφησης να μπορεί να υπολογιστεί από το κλειδί αποκρυπτογράφησης και αντίστροφα. Οι αλγόριθμοι αυτοί καλούνται **συμμετρικοί αλγόριθμοι** ή αλγόριθμοι μυστικού κλειδιού (σχήμα 1). Στους περισσότερους συμμετρικούς αλγόριθμους, το κλειδί κρυπτογράφησης είναι το ίδιο με το κλειδί αποκρυπτογράφησης.

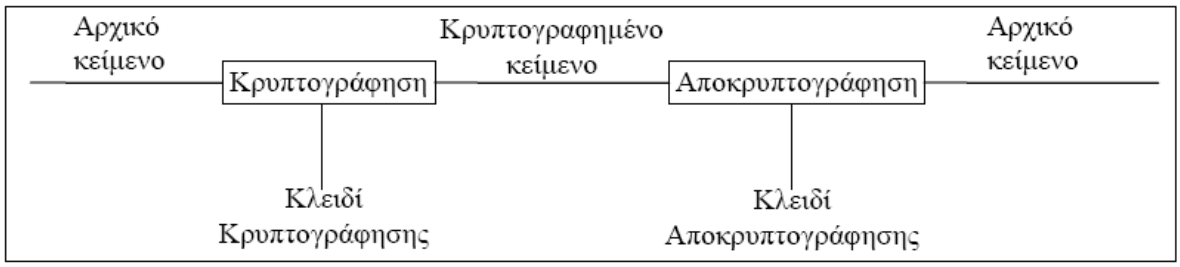


Σχήμα 1 Σύστημα μυστικού κλειδιού

Αλγόριθμοι δημοσίου κλειδιού

Οι αλγόριθμοι δημόσιου κλειδιού (ή συμμετρικοί αλγόριθμοι) είναι σχεδιασμένοι κατά τέτοιον τρόπο ώστε το κλειδί για την κρυπτογράφηση να διαφέρει από το κλειδί της αποκρυπτογράφησης. Επίσης, το κλειδί αποκρυπτογράφησης δεν μπορεί να υπολογιστεί από το κλειδί κρυπτογράφησης. Οι αλγόριθμοι αυτοί, καλούνται **δημοσίου κλειδιού,** επειδή το κλειδί κρυπτογράφησης μπορεί να είναι δημόσιο (public): ένας ξένος μπορεί να χρησιμοποιήσει το κλειδί κρυπτογράφησης (δημόσιο κλειδί) για να κρυπτογραφήσει ένα μήνυμα, αλλά μόνο ένας συγκεκριμένος άνθρωπος με το αντίστοιχο κλειδί αποκρυπτογράφησης (ιδιωτικό κλειδί), μπορεί να αποκρυπτογραφήσει το μήνυμα (σχήμα 2). Το κρυπτογραφημένο μήνυμα καλείται και **κρυπτογράφημα**.

Ορισμένες φορές, τα μηνύματα κρυπτογραφούνται με το ιδιωτικό κλειδί, και αποκρυπτογραφούνται με το δημόσιο κλειδί. Αυτή η μέθοδος χρησιμοποιείται στις ψηφιακές υπογραφές, όπου υπογραφή = κρυπτογράφηση και πιστοποίηση = αποκρυπτογράφηση.



Σχήμα 2 Σύστημα δημόσιου κλειδιού

2.2.1 Διαχείριση κλειδιού

Η διαχείριση κλειδιών αποτελεί ίσως τη δυσκολότερη εργασία στον τομέα της κρυπτογραφίας. Η κακή διαχείριση είναι συνήθως η αιτία που καταρρέουν τα περισσότερα συστήματα, ακόμα και αν βασίζονται στους ισχυρότερους αλγόριθμους:

- **Δημιουργία του κλειδιού**
  - **Κακή επιλογή κλειδιού:** ένα κλειδί δεν πρέπει να είναι κοινότυπο. Εαν ναι, τότε είναι ευάλωτο σε επιθέσεις λεξικού (dictionary attack), όπου ο επιτιθέμενος χρησιμοποιεί ένα λεξικό με κοινές λέξεις
  - **Τυχαιότητα του κλειδιού:** Τα "καλά" κλειδιά, είναι αλφαριθμητικά τυχαίων bits, τα οποία δημιουργούνται από κάποια αυτόματη επεξεργασία. Κάθε bit ενός τυχαίου κλειδιού πρέπει να είναι εξίσου πιθανό .

- **Μεταφορά του κλειδιού:** Ιδίως στα μεγάλα δίκτυα, ο τρόπος με τον οποίο τα κλειδιά μεταφέρονται ή τίθονται υπό διαπραγμάτευση μεταξύ των χρηστών, πρέπει να είναι ασφαλής. Έχουν προταθεί πολλά πρωτόκολλα ανταλλαγής κλειδιών , η επιλογή ενός εκ των οποίων πρέπει να γίνεται με μεγάλη προσοχή.

- **Αποθήκευση και Ενημέρωση του κλειδιού:** Τα κλειδιά πρέπει να αποθηκεύονται ασφαλώς. Εαν είναι δύσκολο να ανακαλούνται με τη μνήμη, η καλύτερη λύση είναι η αποθήκευσή τους σε μία έξυπνη κάρτα (smart card). Επίσης, τα κλειδιά πρέπει να έχουν μια περίοδο ζωής, δηλαδή να αλλάζουν συχνά, ώστε να μη δίνεται η ευκαιρία στους κρυπταναλυτές να δοκιμάζουν τυχαία κλειδιά για μεγάλο χρονικό διάστημα.

2.2.2 Κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται στο Internet

Υπάρχει ένας μεγάλος αριθμός κρυπτογραφικών αλγορίθμων, κάθε ένας από τους οποίους έχει τα δικά του χαρακτηριστικά, πλεονεκτήματα και μειονεκτήματα. Οι πιο ευρέως χρησιμοποιούμενοι, στους οποίους θα αναφερθούμε και στη συνέχεια του παρόντος, είναι οι ακόλουθοι:

- Το **DES** ή Data Encryption Standard, υϊοθετήθηκε το 1976 ως standard από το NIST (National Institute of Standards and Technology) και είναι συμμετρικός αλγόριθμος. Κρυπτογραφεί ανά τμήματα (blocks) των 64 bits (8 bytes) με 16 επαναλήψεις για κάθε τμήμα, χρησιμοποιώνας ένα κλειδί των 56 bits. Παρά το μεγάλο χρονικό διάστημα που έχει περάσει από την γέννησή του, χρησιμοποιείται κατά κόρον.

- Το **Triple-DES** είναι μια παραλλαγή του DES, και κρυπτογραφεί τρεις φορές το ίδιο κείμενο με τον αλγόριθμο DES, αλλά χρησιμοποιώντας διαφορετικό κλειδί για κάθε κρυπτογράφηση.

- Το **IDEA** ή Internetional Data Encryption Algorithm, αναπτύχθηκε το 1990 και είναι δομημένο όπως το DES. Κρυπτογραφεί τμήματα των 64 bits (με 8 επαναλήψεις για κάθε τμήμα) χρησιμοποιώντας ένα κλειδί μήκους 128 bits. Είναι συμμετρικός αλγόριθμος.

- Το **RSA** είναι ένας αλγόριθμος δημοσίου κλειδιού που αναπτύχθηκε το 1978. Τα κλειδιά μήκους 512 bits που χρησιμοποιεί, δημιουργούνται με την παραγοντοποίηση μεγάλων πρώτων αριθμών (300 ψηφία ή περισσότερα). Το RSA μπορεί να χρησιμοποιηθεί και για ψηφιακή υπογραφή (είναι standard), αντιστρέφοντας απλά τον

τρόπο με τον οποίο χρησιμοποιούνται τα κλειδιά (το ιδιωτικό για αποκρυπτογράφηση και υπογραφή, το δημόσιο για κρυπτογράφηση και πιστοποίηση υπογραφής).

- Το **DSA** ή Digital Signature Algorithm είναι ένας αλγόριθμος που χρησιμοποιείται αποκλειστικά για ψηφιακές υπογραφές και την πιστοποίησή τους. Αναπτύχθηκε το 1991 από το NIST. Ως αλγόριθμος είναι πιο αργός από το RSA.

- Τα **RC2** και **RC4** είναι αλγόριθμοι που αναπτύχθηκαν από τον Ron Rivest (έναν από τους δημιουργούς του RSA). Διαθέτουν κλειδιά μεταβλητού μήκους (από 40 έως 128 bits) και χρησιμοποιούνται σε διάφορα e-mail προγράμματα.

2.2.3 End-to-End και Link-to-Link Κρυπτογράφηση

Όταν χρησιμοποιούνται **end-to-end** συστήματα, τόσο ο αποστολέας όσο και ο παραλήπτης πρέπει να είναι εφοδιασμένοι με κατάλληλο, συμβατό hardware. Αφότου πιστοποιήσει ο ένας τον άλλον, οι δύο χρήστες ανταλλάσουν κρυπτογραφημένη πληροφορία. Τα μηνύματα κρυπτογραφούνται από τον αποστολέα και αποκρυπτογραφούνται μόνο όταν φτάσουν στον τελικό προορισμό τους.

Με τη **link-to-link** κρυπτογράφηση, δεν είναι απαραίτητος ο εφοδιασμός με συγκεκριμένο hardware. Εντούτοις, τα κρυπτογραφημένα μηνύματα μεταβιβάζονται σε μια ακολουθία κόμβων (π.χ routers), κάθε ένας από τους οποίους αποκρυπτογραφεί, διαβάζει και ξανά-κρυπτογραφεί το μήνυμα. Αυτή η μέθοδος είναι περισσότερο ευάλωτη.

2.3 Αυθεντικοποίηση με συστήματα δημοσίου και μυστικού κλειδιού

Ψηφιακή υπογραφή

Ας υποθέσουμε ότι η Alice θέλει να αυθεντικοποιήσει τον Bob. Ο Bob έχει ένα ζεύγος κλειδιών, ένα δημόσιο και ένα ιδιωτικό. Ο Bob αποκαλύπει το δημόσιο κλειδί του στην Alice. Εαν κάποιος καλεί την Alice, και η Alice θέλει δει αν πρόκειται όντως για τον Bob και όχι για κάποιον άλλον, η Alice μπορεί να χρησιμοποιήσει την μη συμμετρική φύση της κρυπτογράφησης δημόσιου κλειδιού. Η Alice στέλνει ένα τυχαίο μήνυμα στον Bob και ο Bob απαντάει κρυπτογραφώντας το μήνυμα, χρησιμοποιώντας το ιδιωτικό κλειδί του.

Η Alice λαμβάνει το μήνυμα και το αποκρυπτογραφεί χρησιμοποιώντας το δημόσιο κλειδί του Bob (που έλαβε πριν). Μπορεί να συγκρίνει το μήνυμα αυτό με το αρχικο μήνυμα που έστειλε, και αν ταιριάζουν, γνωρίζει ότι μιλάει με τον Bob. Ένας "απατεώνας" δεν γνωρίζει το ιδιωτικό κλειδί του Bob, οπότε δεν μπορεί να κρυπτογραφήσει το τυχαίο μήνυμα που στέλνει η Alice.

Δεν είναι καλή ιδέα για κάποιον να κρυπτογραφεί κάτι με το ιδιωτικό του κλειδί, εκτός και αν γνωρίζει ακριβώς τί υπογράφει. Αυτό ισχύει διότι το κρυπτογραφημένο μήνυμα ενδέχεται να χρησιμοποιηθεί εναντίον του, με διάφορους τρόπους. Γι'αυτό, αντί να κρυπτογραφήσει το μήνυμα που του έστειλε η Alice, ο Bob δημιουργεί μια hash τιμή του μηνύματος (message digest) και κρυπτογραφεί αυτή. Χρησιμοποιώντας ένα digest, ο Bob μπορεί να προστατεύσει τον εαυτό του. Υπολογίζει το digest του μηνύματος που πήρε από την Alice, και κρυπτογραφεί το αποτέλεσμα. Στην συνέχεια στέλνει το κρυπτογράφημα στην Alice. Η Alice υπολογίζει ομοίως το digest του μηνύματος που είχε στείλει, αποκρυπτογραφεί το μήνυμα του Bob, και αυθεντικοποιεί τον Bob συγκρίνοντας τις δύο hash τιμές.

Η τεχνική που περιγράφτηκε προηγουμένως είναι γνωστή και ως **ψηφιακή υπογραφή**. Ο Bob υπέγραψε το μήνυμα που έλαβε από την Alice. Αυτό όμως, είναι

περίπου το ίδιο επικίνδυνο με την κρυπτογράφηση ενός τυχαίου μηνύματος που προέρχεται από την Alice. Συνεπώς, το πρωτόκολλο αυθεντικοποίησης που προτείνουμε χρειάζεται την αποστολή από τον Bob κάποιων επιπλέον δεδομένων:

A✎B	Γειά, είσαι ο Bob;
B✎A	Alice, Εδώ Bob
	{ digest [Alice, εδώ Bob] } ιδιωτικό-κλειδί-Bob

Χρησιμοποιώντας αυτό το πρωτόκολλο, ο Bob γνωρίζει τί μήνυμα στέλνει στην Alice, και δεν τον ενοχλεί να το υπογράψει. Πρώτα στέλνει το μη κρυπτογραφημένο μήνυμα "Alice, εδώ Bob" και στη συνέχεια στέλνει το κρυπτογραφημένο digest του μηνύματος. Έτσι, η Alice μπορεί εύκολα να πιστοποιήσει ότι ο Bob είναι ο Bob, και ο Bob δεν έχει υπογράψει κάτι που δεν ήθελε.

Γνωστοποίηση του δημόσιου κλειδιού

Πώς παραδίδει όμως ο Bob το δημόσιο κλειδί του στην Alice, κατά ασφαλή τρόπο; Ας πούμε ότι το πρωτόκολλο αυθεντικοποίησης έμοιαζε ως εξής:

A✎B	Γεια
B✎A	Γειά, Είμαι ο Bob, δημόσιο-κλειδί-Bob
A✎B	Απέδειξέ το
B✎A	Alice, Εδώ Bob
	{ digest [Alice, Εδώ Bob] } ιδιωτικό-κλειδί-Bob

Με αυτό το πρωτόκολλο, οποιοσδήποτε μπορεί να είναι ο Bob. Το μόνο που χρειάζεται κάποιος, είναι ένα ζεύγος κλειδιών (δημόσιο και ιδιωτικό). Λέγοντας ψέμματα στην Alice ότι είναι ο Bob, και παρέχοντας της το δικό του δημόσιο κλειδί αντί για του Bob, κάποιος μπορεί να εξαπατήσει την Alice. Στη συνέχεια κρυπτογραφεί κάτι με το ιδιωτικό του κλειδί και το στέλνει στην Alice, οπότε η Alice δεν μπορεί να φανταστεί ότι δε μιλάει στην πραγματικότητα με τον Bob.

Πιστοποιητικά

Προκειμένου να λύσει αυτό το πρόβλημα, η κοινότητα των standards ανακάλυψε ένα αντικείμενο που λέγεται πιστοποιητικό (certficate). Σε ένα πιστοποιητικό, υπάρχουν τα εξής:

- Το όνομα του εκδότη του πιστοποιητικού
- Το όνομα του υποκειμένου για το οποίο εκδίδεται το πιστοποιητικό
- Το δημόσιο κλειδί του υποκειμένου
- Η περίοδος ισχύος του πιστοποιητικού
- Ένας σειριακός αριθμός (για διαχειριστικούς λόγους)

Το πιστοποιητικό είναι υπογεγραμμένο με το ιδιωτικό κλειδί του εκδότη του. Όλοι γνωρίζουν το δημόσιο κλειδί του εκδότη ενός πιστοποιητικού. Τα πιστοποιητικά είναι ένας standard τρόπος σύνδεσης ενός **δημόσιου κλειδιού** με ένα **όνομα**.

Χάρη στην τεχνολογία των πιστοποιητικών, οποιοσδήποτε μπορεί να εξετάσει το πιστοποιητικό του Bob, ώστε να δει εαν είναι παραβιασμένο ή όχι. Υποθέτωντας ότι ο Bob διαχειρίζεται σωστά το ιδιωτικό του κλειδί, και είναι πραγματικά ο Bob όταν λαμβάνει το πιστοποιητικό, τότε δεν υπάρχει κανένα πρόβλημα. Το προτεινόμενο πρωτόκολλο είναι το εξής:

A✎B Γεια
B✎A Γεια, Εδώ Bob, πιστοποιητικό-Bob
A✎B Απέδειξέ το
B✎A Alice, Εδώ Bob
{ digest [Alice, Εδώ Bob] } ιδιωτικό-κλειδί-Bob

Όταν η Alice λάβει το πρώτο μήνυμα του Bob, μπορεί να εξετάσει το πιστοποιητικό, να ελέγξει την υπογραφή και έπειτα να ελέγξει το όνομα του υποκειμένου ώστε να διαπιστώσει αν πράγματι είναι ο Bob. Έπειτα μπορεί να βεβαιωθεί ότι το δημόσιο κλειδί είναι του Bob, και να ζητήσει από τον Bob να αποδείξει την ταυτότητά του. Ο Bob κάνει ό,τι ακριβώς και προηγουμένως, υπολογίζοντας το digest ενός δικού του μηνύματος και στέλνοντας στην Alice την υπογεγραμμένη εκδοχή του μηνύματος. Η Alice μπορεί να την πιστοποιήσει (την υπογραφή) με το δημόσιο κλειδί που βρήκε στο πιστοποιητικό, και να ελέγξει το αποτέλεσμα.

Ένας κακός τύπος, ο Mallet, θα μπορούσε να κάνει τα εξής:

A✎M Γεια
M✎A Γεια, Εδώ Bob, πιστοποιητικό-Bob
A✎M Απέδειξέ το
M✎A ???

Ο Mallet δεν μπορεί να ικανοποιήσει την Alice στο τελευταίο μήνυμα, εφόσον δεν έχει το ιδιωτικό κλειδί του Bob.

Ασφάλεια στο Internet

Πώς όλα αυτά εφαρμόζονται στο Internet; Εφόσον η Alice αυθεντικοποιήσει τον Bob, μπορεί να κάνει κάτι άλλο. Μπορεί να στείλει στον Bob ένα μήνυμα που μόνο ο Bob μπορεί να αποκωδικοποιήσει:

A✎B {μυστικό} δημόσιο-κλειδί-Bob

Το "**μυστικό"** μπορεί να γίνει γνωστό μόνο με την αποκρυπτογράφηση του μηνύματος με το ιδιωτικό κλειδί του Bob. Έτσι, ακόμα και αν η επικοινωνία του Bob με την Alice παρακολουθείται, μόνο ο Bob μπορεί να λάβει το "μυστικό".

Το "μυστικο" μπορεί να χρησιμοποιηθεί **ως ένα άλλο κλειδί**, αυτήν τη φορά με τη χρήση ενός συμμετρικού αλγόριθμου (όπως DES, RC4, IDEA, κ.λ.π). Η Alice γνωρίζει το μυστικό εφόσον το δημιούργησε πριν το στείλει στον Bob. Ο Bob γνωρίζει το μυστικό εφόσον αποκρυπτογραφεί το μήνυμα της Alice με το ιδιωτικό του κλειδί. Εφόσον και οι δύο γνωρίζουν το μυστικό, μπορούν να χρησιμοποιήσουν ένα συμμετρικό αλγόριθμο και να αρχίσουν να στέλνουν μηνύματα κρυπτογραφημένα με αυτόν.

2.4 Πιστοποιητικά στο Web

Με την εμφάνιση της τεχνολογίας των ψηφιακών πιστοποιητικών, λύθηκε ή τείνει προς τη λύση του ένα από τα μεγαλύτερα ίσως προβλήματα στον τομέα της αυθεντικοποίησης στο Web. Έως τώρα, η ασφάλεια στο Web βασίζονταν κυρίως στη φιλοσοφία της εισαγωγής, εκ μέρους του χρήστη, ενός ID και ενός password. Καθώς όμως οι επιχειρήσεις διευρύνονται, τα Web sites εξελίσσονται και η διαχείρισή τους από έναν απομακρυσμένο υπολογιστή είναι πλέον απαραίτητη, οι εως τώρα μέθοδοι αυθεντικοποίησης "πονοκεφάλιαζαν" τους διαχειριστές δικτύων και τους υπεύθυνους

των εταιριών. Τα πιστοποιητικά είναι ένας ασφαλής και εύκαμπτος τρόπος πιστοποίησης ταυτότητας.

Αφότου κάποιος προμηθευτεί ένα πιστοποιητικό, επισκέφτεται ένα site και αντί να πληκτρολογεί το όνομα και το συνθηματικό του, παρουσιάζει το πιστοποιητικό του στον Web server αποδεικνύοντας την ταυτότητά του και αποκτώντας έτσι πρόσβαση σε συγκεκριμένους πόρους στο site. Οι χρήστες δε χρειάζονται πλέον να θυμούνται ονόματα και συνθηματικά, όπως και το προσωπικό τεχνικής υποστήριξης ενός δικτύου δε χρειάζεται να βοηθήσει χρήστες που, σε αντίθετη περίπτωση, θα το "απασχολούσαν" ισχυριζόμενοι ότι έχουν ξεχάσει το συνθηματικό τους.

Σήμερα, οι δύο πιο δημοφιλείς browsers αυτην τη στιγμή, ο Netscape Communicator και ο Internet Explorer και ενσωματόνουν την τεχνολογία των πιστοποιητικών στις υλοποιήσεις τους

Όπως έχουμε ήδη αναφέρει, η αυθεντικοποίηση με τη χρήση ψηφιακών πιστοποιητικών δεν είναι απαραίτητα μονομερής, αλλά μπορεί να γίνει και διμερής. Δηλαδή, εκτός από τον client που αυθεντικοποιείται δίνοντας στον server το πιστοποιητικό του, και ο server μπορεί να παρουσιάσει το πιστοποιητικό του στον client.

Διαχείριση των κλειδιών και πιστοποιητικών με hardware

Όταν ένας χρήστης αποκτήσει ένα ψηφιακό πιστοποιητικό, αυτό αποθηκεύεται στο σκληρό δίσκο του υπολογιστή του. Αυτό ισχύει και για το ζεύγος κλειδιών που διαθέτει ένας χρήστης, όταν χρησιμοποιεί κάποιο από τα δημοφιλή πρωτόκολλα αυθεντικοποίησης στο Web, όπως το SSL, που θα εξεταστεί παρακάτω. Το ζεύγος κλειδιών προστατεύεται με συνθηματικό (password) στο τοπικό σύστημα αρχείων, ενώ το πιστοποιητικό αποθηκεύεται συνήθως με την κανονική του μορφή, αφού περιέχει δημόσια πληροφορία. Τόσο η κρυπτογράφηση, όσο και η αποκρυπτογράφηση επαφίενται σε κατάλληλο software.

Εντούτοις, ένας μηχανισμός διαχείρισης πιστοποιητικών και κλειδιών βασισμένος σε hardware θα ήταν περισσότερο ασφαλής και αποτελεσματικός. Ένας τέτοιος μηχανισμός ενδεχομένως να είναι μια **έξυπνη κάρτα** (smart card) ή μια **συσκευή πιστωτικών καρτών** (credit card device), που θα μπορούν να δημιουργήσουν και να αποθηκεύσουν ζεύγη κλειδιών και πιστοποιητικά. Έξυπνες κάρτες προηγμένης τεχνολογίας μπορούν ακόμα και να πραγματοποιήσουν κρυπτογράφηση και αποκρυπτογράφηση με απόδοση πολύ καλύτερη από αυτήν των αντίστοιχων software μηχανισμών. Τα πλεονεκτήματα λοιπόν των μηχανισμών που βασίζονται σε hardware είναι:

- **Αυξημένη ασφάλεια**. Τα ζεύγη κλειδιών δημιουργούνται από μια συσκευή hardware, η οποία καταρχήν έχει περισσότερο αξιόπιστους γεννήτορες τυχαίων αριθμών από ό,τι οι ψευδο-τυχαίοι γεννήτορες τυχαίων αριθμών που βασίζονται σε software. Επιπλέον, εφόσον τα κλειδιά δεν βγαίνουν ποτέ εκτός της κάρτας, είναι άτρωτα σε επιθέσεις.

- **Καλύτερη απόδοση**. Ορισμένες εξειδικευμένες έξυπνες κάρτες περιέχουν μικροεπεξεργαστές κρυπτογράφησης (encryption chips) που παρουσιάζουν καλύτερα αποτελέσματα από τις software υλοποιήσεις.

- **Οι χρήστες μπορούν να χρησιμοποιήσουν οποιοδήποτε διαθέσιμο σταθμό εργασίας.** Εαν οι υπολογιστές σε ένα δίκτυο που διαθέτουν αναγνώστες καρτών είναι περισσότεροι του ενός, ο χρήστης μπορεί να αυθεντικοποιήσει τον εαυτό του από οποιονδήποτε διαθέσιμο υπολογιστή.

2.4 Πρωτόκολλα ασφαλής επικοινωνίας στο Internet

Σήμερα υπάρχουν πολλά πρωτόκολλα που υπόσχονται ασφαλή μετακίνηση των δεδομένων μεταξύ δικτύων . Για το Web, οι administrators μπορούν να επιλέξουν μεταξύ του **Secure Sockets layer** (SSL) και του **Secure HyperText Transport Protocol** (S-HTTP). Τα πρωτόκολλα για online εμπόριο και οικονομικές συναλλαγές, περιλαμβάνουν το **Secure Electronic Transaction** (SET) και το **Private Communication Technology** (PCT). Για δημιουργούς εφαρμογών, τα πρωτόκολλα που δεσπόζουν είναι το **Simple Public Key Mechanism** (SPKM) και το **Generic Security Services** (GSS), ή ακόμα και το TCP/IP.

Δυστυχώς, παρότι τα πρωτόκολλα αυτά έχουν βοηθήσει προς την κατεύθυνση της ασφαλής μετακίνησης δεδομένων, η διαφορετικότητά τους καθιστά δύσκολη την επιλογή ενός εξ'αυτών, όπως και ενίοτε την υλοποίησή τους.

Παρότι τα περισσότερα πρωτόκολλα προσφέρουν τις ίδιες υπηρεσίες -- πιστοποίηση, κρυπτογράφηση και αυθεντικοποίηση -- και χρησιμοποιούν σχεδόν τους ίδιους κρυπτογραφικούς αλγόριθμους, κάθε πρωτόκολλο λειτουργεί σε διαφορετικές εφαρμογές, οπότε και προσφέρει διαφορετικές λύσεις.

Για μια εταιρία που ασχολείται με online εφαρμογές στο Web, υπάρχουν όπως είπαμε δύο επιλογές: το S-HTTP και το SSL. Το **S-HTTP** ως πρωτόκολλο βασίζεται στη κρυπτογραφία δημόσιου κλειδιού, και "ασφαλίζει" το HTTP μεταξύ ενός Web browser και ενός Web server. Αυτό επιτρέπει σε forms-based δεδομένα (που εισέρχονται σε μια φόρμα), να διασχίσουν το Internet ή ένα intranet σε κρυπτογραφημένη μορφή.

Για περισσότερη ασφάλεια (εκτός του HTTP) σε ένα Web περιβάλλον, υπάρχει το πρωτόκολλο **SSL** , το οποίο είναι ενσωματωμένο στην πλειοψηφία των browsers. Το SSL θεωρείται πιο ασφαλές από το S-HTTP γιατί δεν ασφαλίζει τις συνδέσεις στο HTTP επίπεδο, αλλά στο IP-sockets επίπεδο. Αυτό σημαίνει ότι το SSL μπορεί να κρυπτογραφήσει, να αυθεντικοποιήσει και να πιστοποιήσει όλα τα πρωτόκολλα που υποστηρίζονται από έναν Web browser με SSL δυνατότητες, όπως ftp, telnet, E-mail κ.λ.π.

Τα SSL και S-HTTP δεν είναι αμοιβαίως αποκλειστικά, ούτε ανταγωνίζονται μεταξύ τους απαραίτητα. Και τα δύο μπορούν να ενσωματωθούν σε μια Web εφαρμογή, παρέχοντας σημαντική ασφάλεια.

Καμία τεχνολογία δεν είναι άτρωτη σε παραβιάσεις. Για συναλλαγές που παρέχουν ρουτίνες αυθεντικοποίησης και κρυπτογράφησης υλοποιώντας online εμπόριο με πιστωτικές κάρτες, το πρωτόκολλο **PCT** της Microsoft είναι μια αρκετά ασφαλής λύση. Όπως το SSL, έτσι και το PCT είναι διάφανο στους χρήστες και υποστηρίζεται από ευρέως χρησιμοποιούμενες εφαρμογές, όπως ο Internet Explorer.

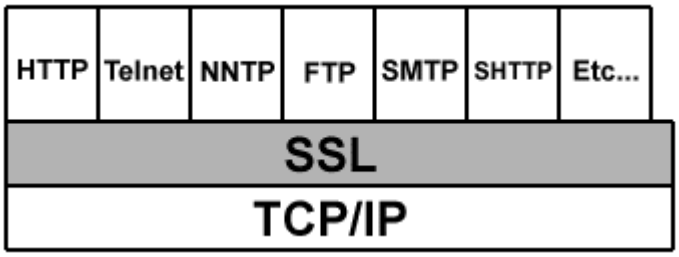
Λιγότερο διαδεδομένο, αλλά όχι λιγότερο αποτελεσματικό είναι το πρωτόκολλο SET, που αναπτύχθηκε από τις Visa International και MasterCard International Inc. Το SET παρέχει στους online τραπεζικούς πελάτες ένα ασφαλές περιβάλλον για οικονομικές συναλλαγές. Το GSS-API είναι ένα language independent (ανεξάρτητο-με γλώσσα - προγραμματισμού) interface το οποίο επιτρέπει στους δημιουργούς εφαρμογών να ενσωματώσουν σε εφαρμογές δικτύων ισχυρές τεχνολογίες κρυπτογράφησης και αυθεντικοποίησης, όπως το **Kerberos.**

Στον πίνακα που ακολουθεί, αναγράφονται τα περισσότερο διαδεδομένα πρωτόκολλα, με τα πλεονεκτήματα και τα μειονεκτήματά τους.

Πρωτόκολλο	Σκοπός	Περιβάλλον	Συνεργασία με	Υπέρ	Κατά
S-HTTP	Ασφάλεια κίνησης στο HTTP επίπεδο	Web browsers	SSL, PCT	Ασφαλίζει μεμονομένη πληροφορία σε μια σελίδα	Δεν υποστηρίζεται αρκετά από τις εταιρίες
SSL	Ασφάλεια στο επίπεδο δικτύου (όλης της κίνησης)	Web browsers και άλλες ανεξάρτητες εφαρμογές	S-HTTP, PCT	Σχετίζεται με πολλά Web πρωτόκολλα	Μεγάλα κλειδιά ✐ προβλήματα απόδοσης
PCT	Ασφάλεια για online οικονομικές συναλλαγές	Web browsers και vendor-specific εφαρμογές	SSL, S-HTTP	extensions ασφαλείας που βελτιώνουν αυτά του SSL	Υποστηρίζεται κυρίως από τη Microsoft
SET	Ασφάλεια για online οικονομικές συναλλαγές	Web browsers και vendor-specific εφαρμογές	SSL, S-HTTP	Εγγενείς μηχανισμοί ασφάλειας συναλλαγών	Άρρηκτα δεμένο με vendor-specific υπηρεσίες
Ipsec	Ασφάλεια της TCP/IP κίνησης για κάθε εφαρμογή	Routers και client software	S/Mime, και άλλες εφαρμογές	Πολύ γρήγορο και ασφαλίζει όλη την κίνηση δικτύου	Πρέπει να υποστηρίζεται από hardware όλων των συμμετέχοντων

2.5.1 Το πρωτόκολλο SSL

Το SSL είναι ένα πρωτόκολλο που χρησιμοποιεί κυρίως την τεχνολογία δημόσιου κλειδιού. Σκοπός του είναι η προστασία (ενθυλάκωση) πρωτοκόλλων υψηλότερου επιπέδου, καθώς εαν θέλουμε να το τοποθετήσουμε στην ιεραρχία των πρωτοκόλλων, βρίσκεται ακριβώς επάνω από το επίπεδο δικτύου και κάτω από το επίπεδο εφαρμογής.



Χρησιμοποιείται ευρέως σε intranets αλλά και στο Internet, στο πλαίσιο επικοινωνίας SSL-ικανών servers και clients. Υποστηρίζεται από μια μεγάλη γκάμα εταιριών στο Internet, όπως επίσης και από public-domain προϊόντα.

Οι υπηρεσίες που παρέχει το SSL, και που μπορούν να χρησιμοποιηθούν από διαφορετικές εφαρμογές, είναι οι ακόλουθες:

Υπηρεσία	Τεχνολογία	Προστασία εναντίον
Ιδιωτικότητα μηνύματος (privacy)	Κρυπτογράφηση	Παρεμβολέων
Ακεραιότητα μηνύματος (integrity)	MACs	"Βανδάλων"
Αμοιβαία αυθεντικοποίηση (mutual auth/tion)	X.509 πιστοποιητικά	"Απατεώνων"

- **Ιδιωτικότητα μηνύματος**. Η προστασία του μηνύματος εξασφαλίζεται μεσω κρυπτογράφησης με ιδιωτικό και δημόσιο κλειδί . Όλη η κίνηση ανάμεσα στον SSL server και τον SSL client κρυπτογραφείται με τη χρήση ενός κλειδιού και ενός αλγόριθμου κρυπτογράφησης που τίθεται υπό διαπραγμάτευση κατά τη διάρκεια μιας **SSL χειραψίας** (handshake).

- **Ακεραιότητα μηνύματος**. Το SSL χρησιμοποιεί ένα συνδυασμό μυστικού κλειδιού και ειδικών μαθηματικών συναρτήσεων που καλούνται hash συναρτήσεις.

- **Αμοιβαία αυθεντικοποίηση**. Ο server πείθει τον client για την ταυτότητά του και ο client πείθει τον server για τη δική του ταυτότητα, χάρη σε πιστοποιητικά δημόσιου κλειδιού. Τα πιστοποιητικά ανταλλάσσονται κατά τη διάρκεια του SSL handshake

Προκειμένου να αποδείξει ότι η οντότητα που παρουσιάζει ένα πιστοποιητικό είναι ο νόμιμος ιδιοκτήτης του πιστοποιητικού, το SSL απαιτεί ο κάτοχος του πιστοποιητικού να υπογράψει ψηφιακά κάποια δεδομένα τα οποία ανταλλάσσονται κατά τη διάρκεια του handshake. Τα ανταλλασσόμενα αυτά δεδομένα περιλαμβάνουν και το πιστοποιητικό. Έτσι αποκλείεται η πιθανότητα κάποιος να υποκρίνεται κάποιον άλλον παρουσιάζοντας το πιστοποιητικό του. Το πιστοποιητικό καθ'αυτό δεν αυθεντικοποιεί: αυτό που αυθεντικοποιεί είναι ο συνδυασμός του πιστοποιητικού με το σωστό ιδιωτικό κλειδί.

Αδυναμίες του SSL

Το SSL, επειδή είναι ένα πρωτόκολλο χαμηλού επιπέδου, δεν κάνει τίποτα για να προστατεύσει το χρήστη, εαν έχει παραβιαστεί ο host. Επίσης, εφόσον παραβιαστεί το κλειδί ενός πιστοποιητικού, τότε μπορεί να παραμείνει ως έχει, καθώς δεν υπάρχει εως σήμερα μηχανισμός που να "συμβουλεύεται" το root μιας Αρχής (CA) ώστε να διαπιστωθεί εαν ένα συγκεκριμένο κλειδί έχει ανακληθεί. Πάντως τα κλειδιά έχουν κάποια χρονική διάρκεια ζωής.

Η χρήση του αλγορίθμου RC4 που χρησιμοποιεί το SSL είναι προβληματική. Το RC4 είναι σχετικά καινύριος αλγόριθμος, δεν έχει δοκιμαστεί αρκετά –σε σύγκριση με άλλους αλγόριθμους όπως DES ή IDEA ώστε να είμαστε βέβαιοι για την ασφάλειά του.

Στο SSL, κατά τη διάρκεια της κρυπτογραφημένης επικοινωνίας και μετά το handshake, όταν ένας εκ των συμμετεχόντων στείλει "κακά" MAC δεδομένα, η σύνδεση διακόπτεται. Το γεγονός αυτό δημιουργεί προϋποθέσεις για επιθέσεις άρνησης υπηρεσίας (denial of service). Επίσης, οι *αριθμοί ακουλουθίας* (sequence numbers) που δημιουργούνται κατά τη σύνδεση, θα πρέπει να είναι όσον το δυνατόν περισσότερο τυχαία αρχικοποιημένοι.

Τέλος, θα έπρεπε να υπάρχει ένας τρόπος ώστε οι δύο πλευρές να μπορούν να επαναδιαπραγματεύονται τα κλειδιά που θα χρησιμοποιούν. Αυτό δεν χρειάζεται για ασφάλεια στην HTTP σύνδεση, η οποία ούτως ή άλλως έχει μικρό διάστημα ζωής, αλλά κυρίως για ασφάλεια στις telnet ή ftp συνδέσεις, οι οποίες διαρκούν συνήθως αρκετά περισσότερο.

2.5.2 Το πρωτόκολλο S-HTTP

Η βασική αυθεντικοποίηση στο πρωτόκολλο HTTP συνίσταται στον έλεγχο πρόσβασης που βασίζεται σε UserIDs και passwords. Τα αρχεία στον server περιέχουν λίστες με τους χρήστες και τα passwords τους σε κρυπτογραφημένη μορφή, όπως και λίστες με ομάδες χρηστών (groups), στις οποίες παρέχονται συγκεκριμένα

προνόμια. Το μοντέλο αυτό αυθεντικοποίησης είναι αρκετά "αδύναμο", ενώ ο administrator του server έχει τον πλήρη έλεγχο της κατάστασης. Επιπλέον, η διαχείρισή του σε μεγάλα δίκτυα παρουσιάζει δυσκολίες. Τέλος, τα passwords μεταφέρονται σε "καθαρή" μορφή (in the clear) χωρίς να κρυπτογραφούνται.

Προκειμένου να εξαλειφθούν οι αδυναμίες του HTTP, αναπτύχθηκε το S-HTTP Το πρωτόκολλο S-HTTP ενεργεί στο **επίπεδο εφαρμογής**, εκτελείται ουσιαστικά σαν μια ξεχωριστή εφαρμογή στο επίπεδο του HTTP και παρέχει κρυπτογράφηση, αυθεντικοποίηση και υπογραφή καθώς και οποιονδήποτε συνδυασμό εξ'αυτών. Ένα από τα πλεονεκτήματα του S-HTTP είναι ότι μπορεί να χρησιμοποιηθεί για την κρυπτογράφηση συγκεκριμένων δεδομένων σε μια Web σελίδα. Παράλληλα, το S-HTTP παρέχει έναν απλό μηχανισμό **πρόκλησης-απάντησης** (challenge-response), επιτρέποντας στα δύο συμβαλλόμενα μέρη να βεβαιωθούν για την επικαιρότητα των μηνυμάτων. Έτσι, εαν ένα S-HTTP μήνυμα περιέχει ένα timestamp, ο αποδέκτης του πρέπει να το συμπεριλάβει στην απάντησή του.

Υπογραφή

Για υπογραφές, ως πιθανοί αλγόριθμοι ορίζονται οι RSA και NIST-DSS. Για την πιστοποίηση της υπογραφής, μπορεί να επισυναφθεί ένα πιστοποιητικό στο μήνυμα.

Ανταλλαγή κλειδιού και Κρυπτογράφηση

Για κρυπτογράφηση μεγάλων ποσοτήτων δεδομένων, χρησιμοποιείται συμμετρική κρυπτογραφία. Τα απαραίτητα κλειδιά μπορούν να ανταλλαχθούν με διαφορετικούς τρόπους:

- RSA: το συμμετρικό κλειδί μεταβιβάζεται κρυπτογραφημένο με το δημόσιο κλειδί του παραλήπτη.

- Χρησιμοποιείται ένα προκαθορισμένο κοινό κλειδί επικοινωνίας. Η απαραίτητη για τον καθορισμό του κλειδιού πληροφορία βρίσκεται στις επικεφαλίδες (headers)

- Προσδίδοντας ονόματα σε κλειδιά, τα καινούρια κλειδιά μπορούν να μεταφερθούν κρυπτογραφημένα σε S-HTTP μηνύματα.

- Kerberos: Τα κλειδιά εξάγονται από τα εισητήρια (tickets) του Kerberos.

Ακεραιότητα μηνύματος και Αυθεντικοποίηση του αποστολέα

Για ένα HTTP μήνυμα, προκειμένου να εξασφαλιστεί η ακεραιότητα του μηνύματος και η αυθεντικοποίηση του αποστολέα, υπολογίζεται ένα MAC. Ο καθορισμός του μυστικού κλειδιού μπορεί να επιτευχθεί με τη χρήση του Kerberos, ή με άλλα μέσα.

2.5.3 Το πρωτόκολλο PCT

Το πρωτόκολλο PCT αναπτύχθηκε από τη Microsoft με σκοπό να αποτρέψει την παρεμβολή τρίτων σε συνδέσεις client/server εφαρμογών. Σύμφωνα με το πρωτόκολλο, τουλάχιστον ένας από τους δύο αυθεντικοποιείται (server ή client), ενώ κάθε ένας έχει το δικαίωμα να απαιτήσει την αυθεντικοποίηση του άλλου. Το PCT είναι παρόμοιο με το SSL στη φιλοσοφία του.

Το PCT είναι ανεξάρτητο από το πρωτόκολλο εφαρμογής που χρησιμοποιείται σε μία σύνδεση. Επάνω από το PCT (στην ιεραρχία των πρωτοκόλλων), μπορεί να

βρίσκεται οποιοδήποτε από τα πρωτόκολλα υψηλού επιπέδου (HTTP, FTP, TELNET, κ.λ.π).

Στο PCT πρωτόκολλο, όλα τα δεδομένα μεταδίδονται ως records (εγγραφές) μεταβλητού μήκους, κάθε μια από τις οποίες έχει μια επικεφαλίδα (header). Αυτά τα records χρησιμοποιούνται για να μεταφέρουν τόσο τα μηνύματα του PCT πρωτοκόλλου (handshake, μηνύματα λαθών, μηνύματα διαχείρισης κλειδιού) καθώς και τα μηνύματα με τα δεδομένα της εφαρμογής. Οι ανταλλαγές των records μεταξύ ενός client και του server, ομαδοποιούνται σε "συνδέσεις", οι οποίες με τη σειρά τους ομαδοποιούνται σε "συνόδους" ("sessions"). Κάθε PCT σύνδεση ανήκει σε μια συγκεκριμένη σύνοδο.

Κάθε σύνδεση, στα πλαίσια του πρωτοκόλλου, αρχίζει με ένα handshake (χειραψία). Στη φάση αυτή, ανταλλάσσεται μια σειρά από handshake μηνύματα, τα οποία διαπραγματεύονται ένα (συμμετρικό) κλειδί επικοινωνίας για τη σύνδεση, όπως επίσης και επιτελούν τις απαραίτητες αυθεντικοποιήσεις με βάση πιστοποιημένα μη συμμετρικά (δημόσια) κλειδιά.

Μόλις τελειώσει η μετάδοση των δεδομένων που προέρχονται από το πρωτόκολλο εφαρμογής, όλα τα δεδομένα (ακόμα και τα μηνύματα λάθους ή/και τα μηνύματα διαχείρισης κλειδιού) κρυπτογραφούνται με τη χρήση κλειδιών κρυπτογράφησης που συμφωνήθηκαν στη φάση του handshake. Εκτός από την κρυπτογράφηση και την αυθεντικοποίηση, το πρωτόκολλο PCT πιστοποιεί την ακεραιότητα των μηνυμάτων με τη χρήση ενός MAC. Το PCT "εμπιστεύεται" ένα αξιόπιστο πρωτόκολλο μεταφοράς (το TCP) για τη μεταφορά των PCT records στη φάση του handshake.

2.5.4 Το πρωτόκολλο SET

Το πρωτόκολλο Secure Electronic Transactions χρησιμοποιείται σήμερα ως standard από πολλές τράπεζες και εταιρίες πιστωτικών καρτών, ως ο μόνος τρόπος για ασφαλές ηλεκτρονικό εμπόριο και προστασία των αριθμών πιστωτικών καρτών από κλοπή και εκμετάλλευση .

Το πρωτόκολλο σχεδιάστηκε ώστε να επιτρέπει στους χρήστες του Internet να αγοράζουν προϊόντα από έμπορους στο Web, κατά τέτοιον τρόπο ώστε ο έμπορος να μη βλέπει ποτέ τον κωδικό πιστωτικής κάρτας του πελάτη, και η τράπεζα να μη μαθαίνει ποτέ τί παρήγγειλε ο πελάτης από τον έμπορο. Το SET λοιπόν, ενδυναμώνει το ηλεκτρονικό εμπόριο εξασφαλίζοντας την ιδιωτικότητα των συναλλαγών (θεωρητικά).

Προκειμένου να χρησιμοποιήσουν το SET, οι πελάτες πρέπει να πληκτρολογήσουν τους κωδικούς των πιστωτικών τους καρτών σε ένα ειδικό "wallet" πρόγραμμα στους υπολογιστές τους . Όταν ένας πελάτης επιθυμεί να αγοράσει ένα προϊόν, επιλέγει ένα link ή button, και ο έμπορος (ο server) του στέλνει ένα ειδικό αρχείο με συγκεκριμένο τύπο, που περιγράφει το προϊόν.

- Ο υπολογιστής του πελάτη πέρνει το αρχείο, και υπολογίζει τη hash τιμή του. Ο υπολογιστής του πελάτη κρυπτογραφεί επίσης και τις οδηγίες αγοράς του πελάτη, οι οποίες περιλαμβάνουν τον κωδικό της πιστωτικής κάρτας και άλλες πληροφορίες. Και τα δύο μηνύματα υπογράφονται, κρυπτογραφούνται, και στέλνονται στον έμπορο.
- Ο έμπορος αποκρυπτογραφεί το πρώτο μήνυμα που περιέχει πληροφορίες για το προϊόν που επιθυμεί να αγοράσει ο πελάτης, και στέλνει το άλλο μήνυμα στην τράπεζα.
- Η τράπεζα αποκρυπτογραφεί το μήνυμα που έλαβε, πιστοποιεί τον κωδικό πιστωτικής κάρτας του πελάτη, εξουσιοδοτεί την πληρωμή και στέλνει μια κρυπτογραφημένη απάντηση στον έμπορο.
- Ο έμπορος αποκρυπτογραφεί την απάντηση από την τράπεζα, την πιστοποιεί, και στέλνει μια επιβεβαίωση στον πελάτη.

Το πρωτόκολλο SET, εκτός από τις εταιρίες που το υποστηρίζουν, δεν έχει βρει υποστηρικτές στην κοινότητα των απλών χρηστών. Ίσως αυτό να συμβαίνει επειδή κανένας χρήστης δεν αισθάνεται άνετα με την προοπτική να έχει αποθηκευμένο τον κωδικό της πιστωτικής του κάρτας στο σκληρό δίσκο.

2.5.5 Το πρωτόκολλο IPSec

Το IP Security είναι πρωτόκολλο **επιπέδου Δικτύου** (επίπεδο 3 στο OSI). Έχει προταθεί ως standard από την IETF (Internet Engineering Task Force), και αποτελεί ίσως την μοναδική σοβαρή ελπίδα για καθιέρωση ενός standard στο χώρο των Virtual Private Networks, τα οποία "βασανίζονται" από την έλλειψη αλληλοσυμβατότητας μεταξύ των πρωτοκόλλων και των μηχανισμών που προτείνονται κατά καιρούς από διάφορες εταιρίες . Έτσι, το 1996 ιδρύθηκε ένα consortium από εταιρίες γνωστές στο χώρο του Internet, το Secure Wide Area Network (S/WAN), το οποίο έχει ως σκοπό να καταστήσει το IPSec ένα standard πρωτόκολλο για την υλοποίηση κρυπτογραφικών μηχανισμών σε δρομολογητές, firewalls, αλλά και σε LANs ή hosts που επικοινωνούν μέσω του Internet.

Συγκεκριμένα, το Ipsec προσφέρει υπηρεσίες Ακεραιότητας (integrity), Αυθεντικοποίησης (authentication) και Εμπιστευτικότητας (confidentiality). Το IPSec είναι πρωτόκολλο του IP επιπέδου και βασίζεται στην αρχιτεκτονική ασφαλείας του IP. Το IPSec υλοποιεί δύο κρυπτογραφικούς μηχανισμούς ασφαλείας για το IP:

Ο πρώτος είναι η **IP Επικεφαλίδα Αυθεντικοποίησης** που παρέχει ακεραιότητα και αυθεντικοποίηση για τα IP datagrams, αλλά όχι εμπιστευτικότητα ,αυξάνει επίσης τόσο το υπολογιστικό κόστος επεξεργασίας, αλλά και την υπολογιστική βραδύτητα του δικτύου.

Ο δεύτερος μηχανισμός, το **IP Encapsulating Security Payload** παρέχει ακεραιότητα, αυθεντικοποίηση και εμπιστευτικότητα τόσο σε tsansport, όσο και σε tunnel mode. Σε transport mode, ένα πρωτόκολλο υψηλότερου επιπέδου όπως το TCP ενθυλακώνεται στην επικεφαλίδα του ESP. Σε tunnel mode, το ESP ενθυλακώνει ολόκληρο το IP datagram στην επικεφαλίδα του, κρυπτογραφεί τα περισσότερα από τα περιεχόμενα και έπειτα προσθέτει την IP επικεφαλίδα (header) με την κανονική της μορφή (cleartext), ώστε το πακέτο να δρομολογηθεί κανονικά μέσω του δικτύου.

Διαχείριση κλειδιού

Δύο πρωτόκολλα διαχείρισης κλειδιού μπορούν να υλοποιηθούν με το IPSec: Το ISAKMP/Oakley (Internet Security Association & Key Management Protocol), ή το SKIP (Simple Key Management Protocol). Παρότι το ISAKMP/Oakley έχει επιλεχθεί ως standard, το SKIP εμφανίζεται ως το de facto standard στην αγορά. Το ISAKMP παρέχει το πλαίσιο (framework) για αυθεντικοποίηση και ανταλλαγή κλειδιού, αλλά δεν τα ορίζει, καθώς έχει σχεδιαστεί ώστε να υποστηρίζει πολλές και διαφορετικές ανταλλαγές κλειδιών. Το SKIP, σχεδιάστηκε ώστε να συνεργάζεται με ένα πρωτόκολλο όπως το IP. Επίσης, το SKIP επιτρέπει τη multicast διανομή κλειδιών, και επιτρέπει σε έναν Internet host να στείλει ένα κρυπτογραφημένο μήνυμα σε έναν άλλο host, χωρίς να χρειάζεται να προϋπάρξει επικοινωνία για τη διαπραγμάτευση και ανταλλαγή των κλειδιών κρυπτογράφησης.

Το μέλλον του IPSec: VPN μεταξύ δύο hosts

Το IPSecure υποστηρίζει την ασφαλή επικοινωνία μεταξύ δύο hosts (host-to-host), όπως επίσης μεταξύ δύο LANs (lan-to-lan), εκτός από την client/server επικοινωνία που υποστηρίζουν τα άλλα πρωτόκολλα. Αυτό είναι πολύ σημαντικό από τη

σκοπιά του απλού χρήστη, καθώς στο μέλλον θα είναι εφικτή η δημιουργία ενός VPN – κρυπτογράφηση και αυθεντικοποίηση των επικοινωνιών μεταξύ δύο υπολογιστών που βρίσκονται σε διαφορετικά σημεία στο Internet.

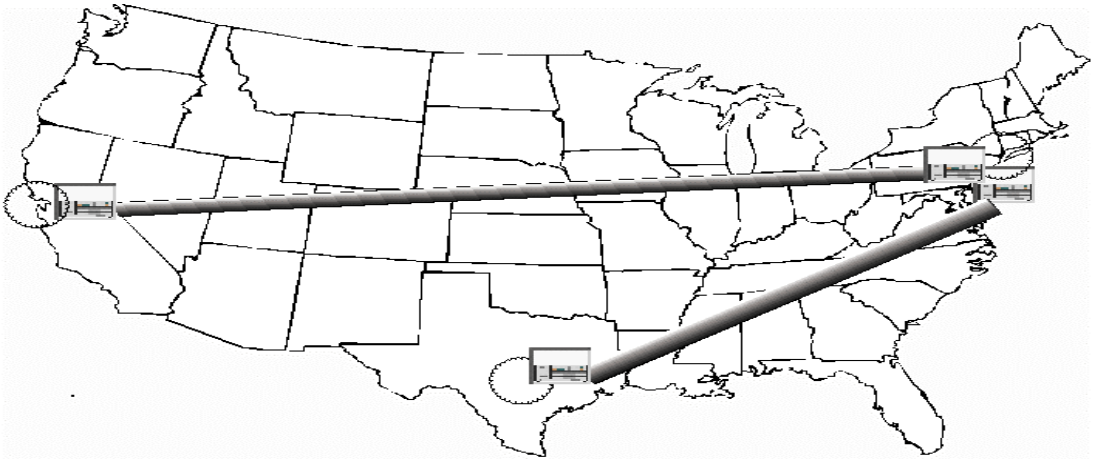
2.5.6 Το πρωτόκολλο PPTP

Το πρωτόκολλο Point-to-Point Tunneling Protocol σχεδιάστηκε από τη Micorsoft στις αρχές του 1996, με σκοπό να παράσχει όλα τα ασφαλή χαρακτηριστικά μιας VPN σύνδεσης. Το PPTP, εαν υλοποιηθεί από τους Internet Service Providers, μπορεί να εξασφαλίσει, για τους χρήστες που έχουν PPP σύνδεση στο Internet μέσω ενός ISP, ασφαλή επικοινωνία με απομακρυσμένους servers.

Το PPTP είναι **επιπέδου Σύνδεσης Δεδομένων** (Data link, επίπεδο 2 στο OSI). Κρυπτογραφεί και ενθυλακώνει τα Point-to-Point Protocol πακέτα (τα μετατρέπει σε PPTP), ώστε να βεβαιώνεται ότι ο χρήστης έχει εξουσιοδοτημένη πρόσβαση στο τοπικό δίκυο, αφετέρου να "παραμορφώνει" τα δεδομένα που στέλνονται ώστε οι outsiders να μη μπορούν να τα καταλάβουν. Η ασφάλεια προσφέρεται σε δύο σημεία. Πρώτον, τα πακέτα από έναν απομακρυσμένο χρήστη αυθεντικοποιούνται από τον ISP. Δεύτερο, εαν η πρόσβαση στο ιδιωτικό δίκτυο ελέγχεται από έναν Windows NT server, τα πακέτα αυθεντικοποιούνται πάλι.

2.6 Virtual Private Networks

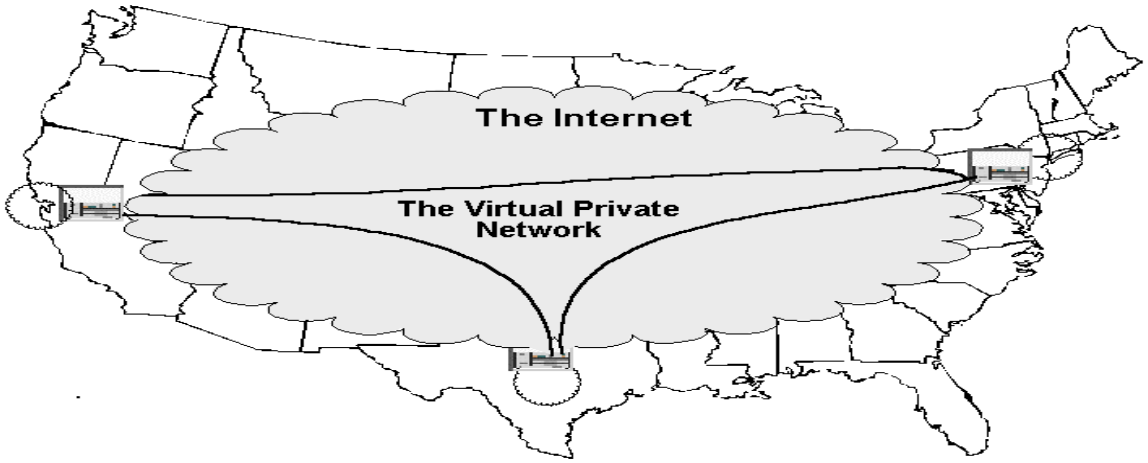
Η μεταφορά μέσω του Internet εμπιστευτικής πληροφορίας, με έναν αξιόπιστο και ασφαλή τρόπο, καλείται Virtual Private Network (Εικονικό Ιδιωτικό Δίκτυο) . Γενικά, το VPN είναι μια διαδικασία ή ρύθμιση τέτοια ώστε το Internet ή το δημόσιο δίκτυο να είναι ασφαλές και να λειτουργεί όπως ένα Ιδιωτικό Δίκτυο (Private Network). Με άλλα λόγια, την ιδιωτικότητα δεν την εξασφαλίζουν τα κυκλώματα (circuits) ή οι μισθωμένες γραμμές (leased lines) ενός Private Network, αλλά οι μηχανισμοί ασφαλείας και οι επεξεργασίες που, στα πλαίσια ενός VPN, επιτρέπουν μόνο σε συγκεκριμένους χρήστες την πρόσβαση σε εμπιστευτικά δεδομένα.



Σχήμα 3 Ένα τυπικό Ιδιωτικό Δίκτυο (PN)

Στο παρελθόν, αλλά και σήμερα, χρησιμοποιούνταν WAN facilities όπως μισθωμένες γραμμές, ώστε να συνδέονται απομακρυσμένα sites της ίδιας εταιρίας ή συνεργαζόμενων εταιριών, όπως φαίνεται και στο σχήμα 3 που απεικονίζει ένα τυπικό PN μεταξύ τριών sites. Τονίζεται ότι για κάθε μισθωμένη γραμμή, χρησιμοποιείται ένα ζεύγος δρομολογητών (που συμβολίζονται με ένα "κουτί").Η εξέλιξη του Internet και του World Wide Web καθώς και η εμφάνιση της τεχνολογίας των Intranets, οδήγησαν τις επιχειρήσεις στο να συνειδητοποιήσουν ότι οι τεχνολογίες του Internet θα μπορούσαν να χρησιμοποιηθούν ώστε να επεκτείνουν ή να αντικαταστήσουν τις client/server εφαρμογές

στα Ιδιωτικά τους Δίκτυα. Το σχήμα 4 αναπαριστάνει το ίδιο "συνεταιρικό" δίκτυο, αλλά αυτήν τη φορά χρησιμοποιούνται οι μηχανισμοί ασφαλείας ενός VPN, με το Internet ως WAN component.



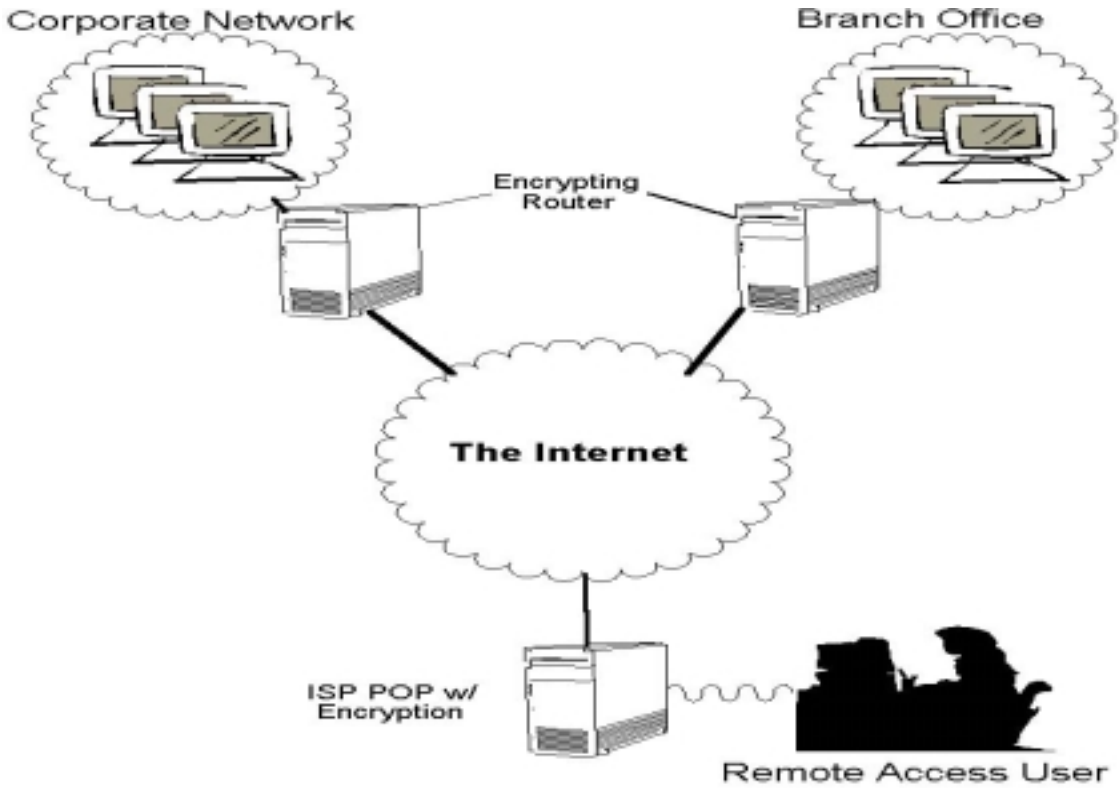
Σχήμα 4

Ένα VPN είναι επιθυμητό για πολλούς λόγους. Καταρχήν, η προσέγγιση των VPNs οδηγεί σε εντυπωσιακή μείωση του κόστους τηλεπικοινωνιών. Εφόσον η "συνδεσιμότητα" (connectivity) στο Internet είναι καθολική, μια σύνδεση υψηλής ταχύτητας προϋποθέτει μόνο μία τοπική μισθωμένη γραμμή.

Επιπλέον, τα VPNs παρουσιάζουν ευκαμψία και επεκτασιμότητα, σε αντίθεση με τα PNs, χάρη στους μηχανισμούς δρομολόγησης στο Internet. Στο PN του σχήματος 4, εαν επιθυμούσαμε να επεκτείνουμε το δίκτυο ώστε να περιλαμβάνει και ένα ακόμα site, τότε θα έπρεπε να παραγγελθεί και να εγκατασταθεί μια επιπλέον μισθωμένη γραμμή. Στο VPN όμως του σχήματος 5, αυτό που θα χρειάζονταν για την προσθήκη του επιπλέον site, θα ήταν ένας επιπλέον δρομολογητής, και κατάλληλη διαμόρφωση των ήδη υπάρχοντων δρομολογητών –απλή εργασία για ένα διαχειριστή δικτύου.

Παρότι υπάρχει ένας μεγάλος αριθμός τεχνολογιών και πρωτοκόλλων που μπορούν να χρησιμοποιηθούν στην υλοποίηση ενός VPN, η πιο κοινή μορφή ενός VPN είναι αυτή που εμπεριέχει ένα encrypting firewall ή έναν encrypting router (δρομολογητής). Το firewall ή ο router δημιουργούν ένα κρυπτογραφημένο "tunnel" ή ασφαλές κανάλι στο Internet. Αυτό το tunnel, μαζί με ένα συμβατικό firewall και άλλους μηχανισμούς ασφαλείας, δημιουργούν μια "εικονική περίμετρο ασφαλείας" (virtual security perimeter) γύρω από το VPN. Το σχήμα 5 δείχνει μια λειτουργική (operational) όψη ενός VPN.

Ο όρος "tunneling" αναφέρεται στη διαδικασία της ενθυλάκωσης (encapsulating) ενός πρωτοκόλλου μέσα σε ένα άλλο πρωτόκολλο, για μεταφορά μέσω ενός δικτύου. Για παράδειγμα, προκειμένου να σταλούν IPX πακέτα μέσω ενός TCP/IP δικτύου, τα IPX πακέτα πρέπει πρώτα να ενθυλακωθούν μέσα σε ένα IP πακέτο. Η τεχνολογία των VPNs επεκτείνει αυτήν την αντίληψη για λόγους ασφαλείας. Τα εμπιστευτικά δεδομένα κρυπτογραφούνται για Ιδιωτικότητα (privacy), Αυθεντικοποίηση (authentication) και Ακεραιότητα (Integrity), ενθυλακώνονται μέσα σε ένα IPX πακέτο και στη συνέχεια ενθυλακώνονται μέσα σε ένα IP πακέτο για τη μεταφορά τους μέσω του Internet.



Σχήμα 5 Μια λειτουργική όψη ενός VPN

Το μεγαλύτερο μειονέκτημα των VPN hardware και software είναι ότι δεν υπάρχουν καθολικά αναγνωρισμένα standards για τεχνικές κρυπτογράφησης και tunneling. Έτσι, δημιουργείται μια κατάσταση όπου οι εξοπλισμοί που χρησιμοποιούν οι κατασκευαστές (manufacturers) δεν είναι συμβατοί μεταξύ τους. Υπάρχουν διάφορα σχήματα, τα οποία ενεργούν τόσο στο επίπεδο Σύνδεσης Δεδομένων, όσο και στο επίπεδο Δικτύου, αλλά και στο επίπεδο Εφαρμογής. Ορισμένα από αυτά απαιτούν επιπλέον συστήματα για κρυπτογράφηση και διαχείριση κλειδιού (key management).

2.7 Ασφάλεια E-mail

Το e-mail αποτελεί ίσως τη δεσπόζουσα τεχνολογία μεταξύ των χρηστών στην κοινότητα του Internet . Παρ'όλα αυτά, πολλοί από αυτούς που ανταλλάσσουν δεκάδες e-mails καθημερινά, δεν έχουν κατανοήσει την ανάγκη, σήμερα περισσότερο απο ποτέ, για ασφαλή επικοινωνία. Το e-mail πρέπει να ανταλλάσσεται κατά τετοιον τρόπο ώστε να εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα του μηνύματος. Η κρυπτογραφία αντιπροσωπεύει ίσως την σημαντικότερη πρακτική ασφαλείας, διαθέσιμη σήμερα στους χρήστες. Όμως, πολλά από τα e-mail προγράμματα που κυκλοφορούν στο Internet, δεν κρυπτογραφούν τα μηνύματα εκτός και αν αυτό ζητηθεί ρητά από το χρήστη. Εντούτοις, υπάρχουν τεχνολογίες όπως το S/MIME και το PGP που μπορούν να χρησιμοποιηθούν προς αυτήν την κατεύθυνση, και τις οποίες θα εξετάσουμε αργότερα.

Ιοί (Viruses)

Οι περισσότεροι ιοί χρειάζονται ένα δυαδικό περιβάλλον για να "κατοικήσουν". Αυτό σημαίνει ότι πολλοί από αυτούς ενσωματώνονται σε .EXE και .COM αρχεία ή τις βιβλιοθήκες τους –DLLs (Dynamic Link Libraries).

Επιπρόσθετα, τα περισσότερα e-mail συστήματα που είναι συνδεδεμένα με το Internet, χρησιμοποιούν έναν gateway μηχανισμό που ελέγχει την διέλευση εισερχόμενων και εξερχόμενων μηνυμάτων.

Γενικά τα gateways επεξεργάζονται τα attachments (επισυνάψεις αρχείων σε e-

mail) αλλά δε τα ελέγχουν για ιούς. Σήμερα όμως, πολλοί πωλητές Anti-virus προϊόντων (Symantec Corp., McAfee Inc., κ.λ.π) συνεργάζονται με πωλητές firewalls αλλά και άλλων προϊόντων ώστε να ενσωματώνουν τις τεχνολογίες τους σε αυτά. Έτσι, υπάρχουν μηχανισμοί, που συνήθως βρίσκονται "πίσω" από ένα firewall, οι οποίοι ελέγχουν (scan) τα εισερχόμενα μηνύματα για ιούς.

E-mail servers

Μια πτυχή του συστήματος ανταλλαγής e-mails που τυγχάνει περιφρόνησης από τους περισσότερους, είναι η ασφάλεια του μηνύματος e-mail όταν αυτό βρίσκεται αποθηκευμένο σε έναν e-mail server ή στον host ενός τελικού χρήστη (end-user). Τα περισσότερα e-mail προϊόντα που είναι διαθέσιμα σήμερα είναι συστήματα που βασίζονται στο client/server μοντέλο: ο χρήστης συντάσσει και διαβάζει μηνύματα σε έναν desktop ή laptop υπολογιστή, ενώ ένας κεντρικό σύστημα server λειτουργεί σαν "ταχυδρομικό γραφείο" που συγκεντρώνει τα εισερχόμενα μηνύματα για το χρήστη καθώς και στέλνει εξερχόμενα μηνύματα του χρήστη σε άλλους servers.

Σε αυτές τις περιπτώσεις, τα e-mail μηνύματα καθ'αυτά παραμένουν για αρκετές ημέρες συνήθως στον server, και για ακόμη περισσότερες ημέρες στους υπολογιστές των χρηστών. Ακόμα και οι πιο ασφαλείς μέθοδοι κρυπτογράφησης που είναι διαθέσιμες σήμερα δε μπορούν να προστατεύσουν ένα μήνυμα αφότου αυτό αποκρυπτογραφηθεί και αποθηκευτεί σε ένα σύστημα, το οποίο εξ'ορισμού είναι μη ασφαλές. Οι έλεγχοι για ασφάλεια που πραγματοποιούνται καθημερινά σε δίκτυα στο Internet, έχουν καταστήσει σαφές ότι τα λιγότερο προστατευμένα και τα πιο ευάλωτα δεδομένα, είναι αυτά που βρίσκονται σε e-mail servers και στους υπολογιστές των χρηστών

Οι χρήστες δε θα πρέπει να βασίζονται μονάχα στα e-mail προγράμματα για την προστασία των μηνυμάτων τους. Θα πρέπει να προστατεύουν τα μηνήματα, αλλά και γενικά όλα τα εμπιστευτικά τους δεδομένα, κυρίως πριν και μετά τη μεταφορά τους. Τα μηνύματα θα πρέπει να προστατεύονται με τη χρήση κρυπτογραφικών μεθόδων, καθ'όλη τη διάρκεια ζωής τους, ενώ πρέπει να ύϊοθετούνται συχνά μέθοδοι backup για την ανάκτηση των μηνυμάτων που έχουν χαθεί/καταστραφεί.

2.7.1 S/MIME

Το S/MIME (Secure Multipurpose Internet Mail Extension) αποτελεί μια τεχνολογία ασφαλής μεταφοράς ηλεκτρονικών μηνυμάτων. Το 1995, ορισμένοι πωλητές software δημιούργησαν S/MIME με σκοπό τη λύση του προβλήματος παραβίασης του e-mail από τρίτους.

Το S/MIME "χτίζει" την ασφάλεια του επάνω από το πρωτόκολλο MIME (βιομηχανικό standard) με βάση ένα σύνολο από κρυπτογραφικά standards, το PKCS (Public Key Cryptography Standards). Το γεγονός ότι το S/MIME δημιουργήθηκε χρησιμοποιώντας άλλα standards, ανοίγει το δρόμο για την ευρεία χρήση του.

Σύμφωνα με τους δημιουργούς του, το S/MIME προσφέρει Ιδιωτικότητα (Privacy), Ακεραιότητα δεδομένων (data Integrity) και Αυθεντικοποίηση (Authentication), σε όσα e-mail προϊόντα που το υποστηρίζουν. Επίσης, η χρήση του S/MIME έχει ήδη επεκταθεί και πέρα από την e-mail τεχνολογία.

Ανατομία του standard

Το S/MIME βασίζεται σε "ισχυρές" κρυπτογραφικές μεθόδους. Χρησιμοποιεί δυο απλές κρυπτογραφικές δομές: τη ψηφιακή υπογραφή και το ψηφιακό"φάκελο". Και οι δύο υλοποιούνται με τη χρήση του RSA κρυπτογραφικού συστήματος δημόσιου κλειδιού. Η ευχρηστία του RSA συνίσταται στο ότι κάθε χρήστης έχει δύο κλειδιά, ένα ιδιωτικό και ένα δημόσιο, κάθε ένα από τα οποία αντιστρέφει αυτό που κάνει το άλλο.

Η **ψηφιακή υπογραφή** είναι διαδικασία δυο βημάτων: Καταρχήν ένας hashing αλγόριθμος επεξεργάζεται το μήνυμα και παράγει το digest του. Όπως το ανθρώπινο δακτυλικό αποτύπωμα, το digest είναι μοναδικό και μπορεί να χρησιμοποιηθεί ώστε να ταυτοποιήσει το έγγραφο. Το digest με τη σειρά του κρυπτογραφείται με το ιδιωτικό κλειδί του αποστολέα. Η ψηφιακή υπογραφή έχει συγκριτικό πλεονέκτημα απέναντι στην χειρόγραφη υπογραφή, επειδή αντιπροσωπεύει τόσο τα περιεχόμενα του μηνύματος όσο και το συγγραφέα.

Για την **πιστοποίηση της υπογραφής**, ο παραλήπτης αποκρυπτογραφεί την υπογραφή με τη χρήση του δημόσιου κλειδιού του αποστολέα. Η αποκρυπτογράφηση "φανερώνει" το digest, το οποίο ο παραλήπτης συγκρίνει με το δικό του (ήδη υπολογισμένο digest. Εαν τα δυο digest δεν είναι ίδια, τότε μπορεί να συμβαίνουν δύο τινα: ή το μήνυμα έχει υπογραφηθεί με ένα λανθασμένο ιδιωτικό κλειδί, είτε κάποιος έχει παραλάξει το μήνυμα. Οι ιδιότητες αυτές ασφαλείας καλούνται *Αυθεντικοποίηση πηγής* (origin Authentication) και *Ακεραιότητα μηνύματος* (message Integrity).

Για την κρυπτογράφηση των περιεχομένων του μηνύματος με στόχο την ιδιωτικότητα, χρησιμοποιείται ένας **ψηφιακός "φάκελος"**. Ο ψηφιακός φάκελος προσφέρει ιδιωτικότητα υπό την έννοια ότι το μήνυμα μπορεί να διαβαστεί μόνο από τον παραλήπτη για τον οποίο προορίζεται και από κανέναν άλλον. Το μήνυμα καθ'αυτό δεν κρυπτογραφείται με RSA, αλλά με ένα συμμετρικό κλειδί κρυπτογράφησης στα πλαίσια ενός αλγόριθμου όπως ο DES ή ο RC2 . Το συμμετρικό κλειδί στη συνέχεια κρυπτογραφείται με το RSA δημόσιο κλειδί του παραλήπτη. Το κρυπτογραφημένο μήνυμα και το κρυπτογραφημένο κλειδί στέλνονται μαζί στον ψηφιακό φάκελο.

Η εμπιστοσύνη του να έχει κάποιος το σωστό δημόσιο κλειδί του παραλήπτη, είναι κρίσιμη σε ένα περιβάλλον δημόσιου κλειδιού. Ας υποθέσουμε το ακόλουθο παράδειγμα: ο χρήστης Α δέχεται ένα e-mail από τον συνεργάτη του Β, στο οποίο ο Β του αναφέρει ότι έχει αλλάξει το δημόσιο κλειδί του, λόγω του ότι έχει προμηθευτεί ένα καινούριο πρόγραμμα e-mail. Αλλά ο Α πώς γνωρίζει ότι ο αποστολέας αυτού του μηνύματος είναι πραγματικά ο συνεργάτης του; τα "μεταμφιεσμένα" e-mail (e-mail spoofing) είναι σύνηθες φαινόμενο πλέον στο Internet. Έτσι, εαν ο Α κρυπτογραφήσει ένα μήνυμα με το δήθεν καινούριο κλειδί του Β, ο μεταμφιεσμένος "κακόβουλος" χρήστης θα μπορεί να διαβάσει e-mail που δεν προορίζεται γι'αυτόν.

Έτσι, υπάρχει η ανάγκη υϊοθέτησης ενός μηχανισμού που θα προσδιορίζει με ασφάλεια τον αληθινό ιδιοκτήτη ενός δημόσιο κλειδιού. Η λύση σε αυτό το πρόβλημα παρέχεται με τα **ψηφιακά πιστοποιητικά.** Ένα πιστοποιητικό ουσιαστικά αντιστοιχεί ένα όνομα με ένα δημόσιο κλειδί. Το πιστοποιητικό καθ'άυτό είναι υπογεγραμμένο από έναν τρίτο ανεξάρτητο παράγοντα, που καλείται Αρχή Πιστοποιητικού (Certificate Authority, CA). Μια CA είναι μια οντότητα που τυγχάνει περισσότερης εμπιστοσύνης από έναν απλό χρήστη, για την υπογραφή δημόσιων κλειδιών. Έτσι, σε κάθε δημόσιο κλειδί αντιστοιχεί ένα ψηφιακό πιστοποιητικό που υπογράφεται από την CA. Στο S/MIME λοιπόν, κάθε χρήστης δίνει το πιστοποιητικό το στον χρήστη που σκοπεύει να του αποστείλει μήνυμα.

Ο προηγούμενος μηχανισμός είναι χρήσιμος όχι μόνο στο Internet, αλλά και στο intranet της επιχείρησης. Ένας "κακόβουλος" υπάλληλος ενδέχεται να προσπαθήσει να εισάγει το δικό του RSA κλειδί δίπλα από το όνομα ενός ανυποψίαστου χρήστη, ώστε να γίνει κάτοχος μηνυμάτων που δεν προορίζονταν γι'αυτόν. Με τη χρήση των πιστοποιητικών, κάτι τέτοιο είναι πολύ δύσκολο.

2.7.2 Pretty Good Privacy

Το σύστημα PGP είναι δημιουργία του P.Zimmermann και παρέχει υπηρεσίες αυθεντικοποίησης και εμπιστευτικότητας για e-mail & εφαρμογές αποθήκευσης αρχείου.

Δημόσια και Ιδιωτικά κλειδιά

Βασική προϋπόθεση για τη λειτουργία του PGP είναι ότι κάθε χρήστης πρέπει να είναι κάτοχος ενός ιδιωτικού κλειδιού και του αντίγραφου του δημόσιου κλειδιού κάθε πιθανού συνομιλητή του. Το PGP διατηρεί έναν κατάλογο με τα δημόσια κλειδιά που οι χρήστες έχουν προμηθευτεί με τον έναν ή τον άλλο τρόπο. Τα κλειδιά αυτά είναι καταχωρημένα σε ένα αρχείο δημόσιου κλειδιού που περιέχει τις ακόλουθες πληροφορίες:

- Το δημόσιο κλειδί
- Το όνομα του ιδιοκτήτη του κλειδιού
- Ένα μοναδικό προσδιοριστή του κλειδιού (key ID)
- Διάφορες άλλες πληροφορίες για τον ιδιοκτήτη του κλειδιού.

Το ιδιωτικό κλειδί κάθε χρήστη καταχωρείται στο αρχείο ιδιωτικού κλειδιού του χρήστη. Όμως, για την προστασία του κλειδιού το PGP ζητάει ένα passphrase το οποίο είναι μια ακολουθία χαρακτήρων. Το passphrase χρησιμοποιείται για τη δημιουργία ενός 128-bit IDEA κλειδιού για την κρυπτογράφηση του ιδιωτικού κλειδιού με τον αλγόριθμο IDEA. Στη συνέχεια, το PGP καταχωρεί το ιδιωτικό κλειδί στο αρχείο ιδιωτικού κλειδιού και διαγράφει το passphrase και το IDEA κλειδί. Το αρχείο περιέχει τις ακόλουθες πληροφορίες:

- Το ιδιωτικό κλειδί κρυπτογραφημένο με το IDEA κλειδί που δημιουργήθηκε από το passphrase
- Το όνομα του χρήστη (user ID)
- Ένα αντίγραφο του αντίστοιχου δημόσιου κλειδιού

Η ανάκτηση του ιδιωτικού κλειδιού γίνεται μετά την πληκτρολόγηση του passphrase το οποίο το PGP χρησιμοποιεί για την αποκρυπτογράφηση του ιδιωτικού κλειδιού χρησιμοποιώντας πάλι τον αλγόριθμο IDEA.

Ψηφιακές υπογραφές

Το πρώτο βήμα για την αποστολή ενός μηνύματος από ένα χρήστη σε έναν άλλο με τη χρήση του συστήματος PGP είναι η διαδικασία της ψηφιακής υπογραφής του μηνύματος. Η διαδικασία αυτή πραγματοποιείται κατά τον ακόλουθο τρόπο:

- Ο αποστολέας δημιουργεί το μήνυμα.
- Το PGP χρησιμοποιεί τη hash συνάρτηση για την παραγωγή ενός 128-bit κώδικα του μηνύματος.
- Ο αποστολέας προσδιορίζει το ιδιωτικό κλειδί που πρόκειται να χρησιμοποιηθεί και παρέχει ένα passphrase ώστε το PGP να αποκρυπτογραφήσει το ιδιωτικό αυτό κλειδί.
- Το PGP κρυπτογραφεί το hash κώδικα του μηνύματος με τον αλγόριθμο RSA και κλειδί το ιδιωτικό κλειδί του αποστολέα και προσαρτά το αποτέλεσμα στο μήνυμα,

ενώ ο προσδιοριστής του αντίστοιχου κλειδιού του αποστολέα προσαρτάται στη ψηφιακή υπογραφή.

Η αντίστροφη διαδικασία που ακολουθείται στο σημείο παραλαβής της ψηφιακής υπογραφής είναι η ακόλουθη:

- Το PGP παίρνει τον προσδιοριστή κλειδιού (key ID) που έχει προσαρτηθεί στη ψηφιακή υπογραφή του μηνύματος και τον χρησιμοποιεί για την απόκτηση του αντίστοιχου δημόσιου κλειδιού από το αρχείο δημόσιου κλειδιού.
- Το PGP χρησιμοποιεί τον αλγόριθμο RSA μαζί με το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφηση και την απόκτηση του hash κώδικα.
- Το PGP δημιουργεί ένα νέο hash κώδικα του μηνύματος και τον συγκρίνει με αυτόν που έχει αποκρυπτογραφηθεί. Εαν οι δυο κώδικες ταιριάζουν το μήνυμα γίνεται αποδεκτό ως αυθεντικό.

Κρυπτογράφηση μηνύματος

Στο PGP κάθε κλειδί επικοινωνίας (session key) χρησιμοποιείται μια μονό φορά και είναι ένας ψευδοτυχαίος αριθμός 128-bit που προσαρτάται στο μήνυμα και μεταδίδεται μαζί του. Για την προστασία του κλειδιού αυτού χρησιμοποιείται ο αλγόριθμος RSA με κλειδί κρυπτογράφησης το δημόσιο κλειδί του παραλήπτη. Έτσι, μετά τη δημιουργία της ψηφιακής υπογραφής και την παραγωγή του hash κώδικα, η διαδικασία στο σημείο αποστολής είναι:

- Το PGP δημιουργεί ένα ψευδοτυχαίο αριθμό 128-bit (session key)
- Το PGP κρυπτογραφεί το μήνυμα χρησιμοποιώντας τον αλγόριθμο IDEA με το κλειδί επικοινωνίας που δημιούργησε.
- Το PGP κρυπτογραφεί το κλειδί επικοινωνίας με τον αλγόριθμο RSA και το δημόσιο κλειδί του παραλήπτη και προσαρτά το αποτέλεσμα στο μήνυμα. Τέλος, ο προσδιοριστής του δημόσιου κλειδιού του παραλήπτη προσαρτάται επίσης στο κρυπτογραφημένο κλειδί επικοινωνίας.

Για την αποκρυπτογράφηση του μηνύματος στο σημείο παραλαβής, η διαδικασία που ακολουθείται είναι:

- Το PGP παίρνει τον προσδιοριστή κλειδιού (key ID) που έχει προσαρτηθεί στο μήνυμα και τον χρησιμοποιεί για την απόκτηση του αντίστοιχου κλειδιού από το αρχείο ιδιωτικού κλειδιού (ένας χρήστης μπορεί να έχει περισσότερα από ένα ιδιωτικά κλειδιά).
- Ο παραλήπτης παρέχει στο PGP ένα passphrase για την αποκρυπτογράφηση του ιδιωτικού του κλειδιού.
- Το PGP χρησιμοποιεί τον αλγόριθμο RSA με το ιδιωτικό αυτό κλειδί για την απόκτηση του κλειδιού επικοινωνίας (session key).
- Το PGP αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας τον IDEA με κλειδί το κλειδί επικοινωνίας.

2.7.3 PGP εναντίον S/MIME

Το 1991 Ο P. Zimmerman έγραψε το πρόγραμμα PGP για κρυπτογράφηση e-mail , και το έθεσε στην υπηρεσία των χρηστών του Internet δωρεάν. Το PGP προσέφερε "κρυπτογράφηση για τις μάζες". Το PGP όμως είχε (και έχει) ένα πρόβλημα από την αρχή της δημιουργίας του: είναι δύσκολο στη χρήση του. Ο Zimmermann και η εταιρία

του προσπαθούν να δημιουργήσουν μια έκδοση του προγράμματος πιο εύκολη στη χρήση, και ένα plug-in για τον Netscape navigator ώστε να καταστήσουν την κρυπτογράφηση διάφανη στο χρήστη. Εντούτοις, τόσο ο Netscape Navigator όσο και ο Microsoft Explorer υποστηρίζουν την τεχνολογία S/MIME για την κρυπτογράφηση των e-mail μηνυμάτων.

Ο χρόνος θα δείξει ποιός θα είναι ο νικητής, στον πόλεμο των standards που έχει ξεσπάσει στο Internet, όχι μόνο για την ασφαλή μετάδοση e-mail, αλλά και για όλες τις προτεινόμενες τεχνολογίες που κατακλύζουν σήμερα το διαδίκτυο.

2.8 Το σύστημα αυθεντικοποίησης kerberos

Το Kerberos είναι μια κατανεμημένη υπηρεσία αυθεντικοποίησης που επιτρέπει σε μια διαδικασία (client) η οποία εκτελείται εκ μέρους ενός υποκειμένου (principal) να αποδείξει την ταυτότητά της σε έναν πιστοποιητή χωρίς να στέλνει στο δίκτυο δεδομένα που θα επέτρεπαν σε έναν hacker ή στον πιστοποιητή να παραστήσουν το υποκείμενο . Το Kerberos παρέχει προαιρετικά ακεραιότητα και εμπιστευτικότητα για δεδομένα που μεταφέρονται από τον client στον server. Καθώς η χρήση του εξαπλώθηκε και σε άλλα περιβάλλοντα, σημειώθηκαν κάποιες αλλαγές στο σύστημα, ώστε να υποστηρίζονται ποικίλες πολιτικές και μοντέλα χρήσης.

Πώς δουλεύει το Kerberos

Το σύστημα αυθεντικοποίησης Kerberos χρησιμοποιεί μια σειρά από κρυπτογραφημένα μηνύματα ώστε να αποδείξει σε έναν πιστοποιητή (verifier) ότι ο client εκτελείται για λογαριασμό ενός συγκεκριμένου χρήστη. Το πρωτόκολλο Kerberos βασίζεται στο πρωτόκολλο αυθεντικοποίησης των Needham και Schroeder, αλλά με κάποιες αλλαγές ώστε να καλύπτει τις ανάγκες του περιβάλλοντος για το οποίο αναπτύχθηκε. Ανάμεσα σε αυτές τις αλλαγές, είναι και η χρήση των timestamps ώστε να μειωθεί ο αριθμός των απαιτούμενων βημάτων για τη βασική αυθεντικοποίηση, η ύπαρξη μιας "υπηρεσίας ενοικίασης εισητηρίων" (**ticket granting service**) ώστε να υποστηρίζεται η συνακόλουθη αυθεντικοποίηση χωρίς επανα-πληκτρολόγηση του password του υποκειμένου, και μια διαφορετική προσέγγιση στη **σταυρωτή αυθεντικοποίηση** (cross-realm authentication), δηλαδή την αυθεντικοποίηση ενός υποκειμένου που είναι καταχωρημένο σε έναν διαφορετικό server αυθεντικοποίησης από ότι ο πιστοποιητής.

Κρυπτογράφηση στο Kerberos

Παρότι, όπως δηλώθηκε, το Kerberos αποδεικνύει ότι ένας client εκτελείται εκ μέρους ενός συγκεκριμένου χρήστη, μια πιο ακριβής δήλωση είναι ότι ο client έχει γνώση ενός κλειδιού κρυπτογράφησης το οποίο είναι γνωστό μονάχα στον χρήστη και τον server αυθεντικοποίησης. Στο Kerberos, το κλειδί κρυπτογράφησης του χρήστη προκύπτει από, και πρέπει να θεωρηθεί ως ένα **password** (στη συνέχεια θα αναφερόμαστε σε αυτό με τον όρο password). Ομοίως, κάθε server εφαρμογής (application server) "μοιράζεται" ένα **κλειδί κρυπτογράφησης** με τον server αυθεντικοποίησης (έτσι θα αποκαλούμε το κλειδί του server).

Η κρυπτογράφηση στην παρούσα υλοποίηση του Kerberos χρησιμοποιεί το Data Encryption Standard (DES). Μια ιδιότητα του DES είναι ότι εαν ένα κρυπτογράφημα αποκρυπτογραφηθεί με το ίδιο κλειδί που χρησιμοποιήθηκε στην κρυπτογράφησή του, τότε εμφανίζεται το αρχικό κείμενο. Εαν χρησιμοποιηθούν διαφορετικά κλειδιά για κρυπτογράφηση και αποκρυπτογράφηση, ή εαν το κρυπτογράφημα παραλλαχτεί, τότε αφενός το αποτέλεσμα δε θα είναι αναγνώσιμο, αφετέρου το checksum στο Kerberos μήνυμα δε θα ταιριάζει με τα δεδομένα. Αυτός ο συνδυασμός της κρυπτογράφησης και

του checksun παρέχει **ακεραιότητα και εμπιστευτικότητα** για τα κρυπτογραφημένα μηνύματα του Kerberos.

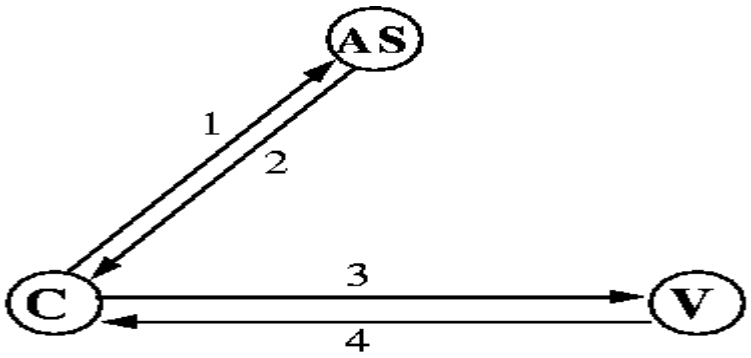
Τα εισητήρια στο Kerberos

Ο client και ο server δεν μοιράζονται εξαρχής ένα κλειδί κρυπτογράφησης. Όποτε ένας client αυθεντικοποιεί τον εαυτό του σε έναν καινούριο πιστοποιητή, βασίζεται στο ότι ο server αυθεντικοποίησης θα δημιουργήσει ένα καινούριο κλειδί κρυπτογράφησης και θα το διανείμει ασφαλώς στα δύο μέρη. Αυτό το καινούριο κλειδί κρυπτογράφησης καλείται *κλειδί επικοινωνίας* (session key) και το εισητήριο (ticket) του Kerberos χρησιμοποιείται για να το παραδώσει στον πιστοποιητή.

Το Kerberos εισητήριο είναι ένα πιστοποιητικό που εκδίδεται από έναν server αυθεντικοποίησης, κρυπτογραφημένο με το κλειδί του server. Μεταξύ άλλων πληροφοριών, το εισητήριο περιλαμβάνει το τυχαίο κλειδί επικοινωνίας που θα χρησιμοποιηθεί για αυθεντικοποίηση του υποκειμένου στον πιστοποιητή, το όνομα του υποκειμένου (principal) για το οποίο εκδόθηκε το κλειδί επικοινωνίας, και ένα χρόνο διαρκείας (expiration time) μετά το πέρας του οποίου το κλειδί επικοινωνίας δεν ισχύει πλέον. Το εισητήριο δεν αποστέλλεται απευθείας στον πιστοποιητή, αλλά πρώτα στον client ο οποίος το προωθεί στον πιστοποιητή, ως τμήμα μιας **αίτησης εφαρμογής** (application request). Επειδή το εισητήριο είναι κρυπτογραφημένο με το κλειδί του server, το οποίο είναι γνωστό μόνο στον server αυθεντικοποίησης και στον αντίστοιχο πιστοποιητή, δεν είναι δυνατόν ο client να τροποποιήσει το εισητήριο χωρίς να ανακαλυφθεί.

Αίτηση εφαρμογής και απάντηση

Τα μηνύματα 3 και 4 στο σχήμα 6 αναπαριστάνουν την αίτηση εφαρμογής (application request) και την απάντηση (response), ίσως την πιο σημαντική ανταλλαγή μυνημάτων στο πρωτόκολλο Kerberos. Μέσω αυτών των μηνυμάτων ο client αποδεικνύει στον πιστοποιητή ότι γνωρίζει το κλειδί επικοινωνίας που είναι ενσωματωμένο στο εισητήριο του Kerberos. Υπάρχουν δυο τμήματα σε μια αίτηση εφαρμογής: ένα εισητήριο και ένας **αυθεντικοποιητής**. Ο αυθεντικοποιητής περιέχει, ανάμεσα στα άλλα, και: την τρέχουσα ώρα, ένα checksum, και ένα προαιρετικό κλειδί κρυπτογράφησης, όλα κρυπτογραφημένα με το κλειδί επικοινωνίας από το συνοδεύων εισητήριο.



1. as_req: c, v, $time_{exp}$, n
2. as_rep: $\{K_{c,v}, v, time_{exp}, n, \ldots\}K_c$, $\{T_{c,v}\}K_v$
3. ap_req: $\{ts,ck, K_{subsession}, \ldots\}K_{c,v}$ $\{T_{c,v}\}K_v$
4. ap_rep: $\{ts\}K_{c,v}$ (optional)

$T_{c,v} = K_{c,v}, c, time_{exp} \ldots$

Σχήμα 6 Βασικό πρωτόκολλο αυθεντικοποίησης στο kerberos (απλοποιημένο)

Μετά από την αίτηση εφαρμογής, ο πιστοποιητής αποκρυπτογραφεί το εισητήριο, αποκτά το κλειδί επικοινωνίας, και χρησιμοποιεί το κλειδί επικοινωνίας ώστε να αποκρυπτογραφήσει τον αυθεντικοποιητή. Το κλειδί με το οποίο αποκρυπτογραφήθηκε ο αυθεντικοποιητής είναι ίδιο με το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφησή του, τότε το checksum θα ταιριάζει και ο πιστοποιητής μπορεί να υποθέσει ότι ο αυθεντικοποιητής δημιουργήθηκε από το υποκείμενο με όνομα αυτό που περιέχεται στο εισητήριο, για τον οποίο εκδόθηκε και το κλειδί επικοινωνίας. Βέβαια, αυτό δεν είναι αρκετό για την αυθεντικοποίηση, εφόσον ένας hacker μπορεί να παρακολουθήσει (sniffing) τον αυθεντικοποιητή και να τον "ξανα-παίξει" αργότερα παριστάνοντας τον χρήστη. Γι'αυτόν το λόγο, ο πιστοποιητής ελέγχει επιπρόσθετα το timestamp ώστε να βεβαιωθεί ότι ο αυθεντικοποιητής είναι επίκαιρος. Εαν το timestamp είναι εντός ενός συγκεκριμένου χρονικού πλαισίου (συνήθως 5 λεπτά) με βάση την ώρα του πιστοποιητή, και εαν το ίδιο timestamp δεν έχει χρησιμοποιηθεί σε άλλες αιτήσεις στο ίδιο χρονικό πλαίσιο, τότε ο πιστοποιητής δέχεται την αίτηση ως αυθεντική.

Μέχρι τώρα η ταυτότητα του client έχει πιστοποιηθεί από τον server. Σε ορισμένες εφαρμογές, ο client επιθυμεί να πιστοποιήσει με τη σειρά του την ταυτότητα του server. Εαν απαιτείται λοιπόν μια **αμοιβαία αυθεντικοποίηση**, ο server δημιουργεί μια απάντηση εφαρμογής (application response) εξάγοντας τον χρόνο t που έχει εισάγει ο client στον αυθεντικοποιητή, και επιστρέφοντάς τον στον client μαζί με άλλες πληροφορίες, όλα αυτά κρυπτογραφημένα με το κλειδί επικοινωνίας.

Αίτηση Αυθεντικοποίησης και απάντηση

Ο client αξιώνει ένα ξεχωριστό εισητήριο και κλειδί επικοινωνίας για κάθε πιστοποιητή με τον οποίο επικοινωνεί. Όταν ο client επιθυμεί να επικοινωνήσει με ένα συγκεκριμένο πιστοποιητή, χρησιμοποιεί τα μηνύματα 1 και 2 του σχήματος 7 (application request and response), ώστε να αποκτήσει ένα εισητήριο και ένα κλειδί επικοινωνίας από τον server αυθεντικοποίησης. Στην αίτηση αυτή, ο client στέλνει στον server την δεδηλωμένη του ταυτότητα, το όνομα του πιστοποιητή, έναν επιθυμητό χρόνο διαρκείας για το εισητήριο, και έναν τυχαίο αριθμό που θα χρησιμοποιηθεί για την αντιστοίχιση της αίτησης με την απάντηση.

Στην απάντησή του, ο server αυθεντικοποίησης επιστρέφει ένα κλειδί επικοινωνίας, τον αντίστοιχο χρόνο διαρκείας (expiration time), τον τυχαίο αριθμό της αίτησης, το όνομα του πιστοποιητή και άλλες πληροφορίες από το εισητήριο, όλα αυτά κρυπτογραφημένα με το password του χρήστη που είναι καταχωρημένο στον server. Επίσης, επιστρέφει ένα εισητήριο που περιέχει παρόμοιες πληροφορίες, και το οποίο πρόκειται αργότερα να προωθηθεί στον πιστοποιητή ως τμήμα μιας αίτησης εφαρμογής. Η αίτηση-απάντηση αυθεντικοποίησης, και η αίτηση-απάντηση εφαρμογής, συνιστούν το βασικό πρωτόκολλο αυθεντικοποίησης στο Kerberos.

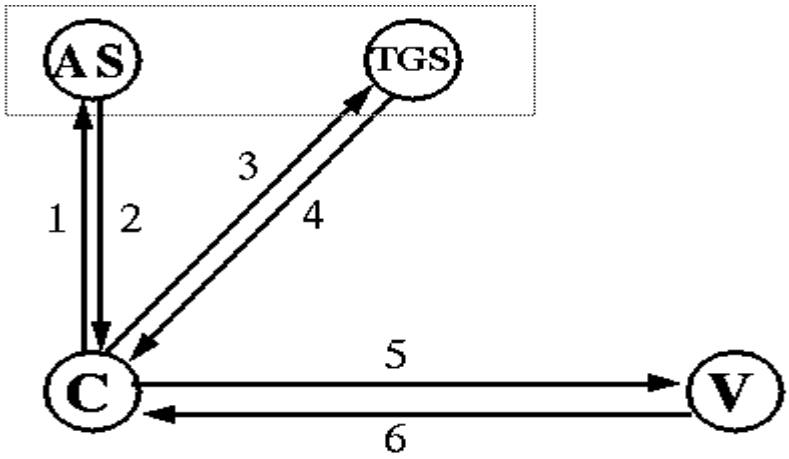
Αποκτώντας επιπρόσθετα εισητήρια

Το βασικό πρωτόκολλο αυθεντικοποίησης, επιτρέπει λοιπόν σε έναν client με τη γνώση του password ενός χρήστη, να αποκτήσει ένα εισητήριο και ένα κλειδί επικοινωνίας ώστε να αποδείξει την ταυτότητά του σε οποιονδήποτε πιστοποιητή που είναι καταχωρημένος στον server αυθεντικοποίησης. Το password του χρήστη πρέπει να παρουσιάζεται κάθε φορά που ο χρήστης αυθεντικοποιείται σε έναν καινούριο πιστοποιητή. Αυτό μπορεί να είναι "άκομψο": αντίθετα, ο χρήστης θα έπρεπε να μπορεί να συνδέεται με το σύστημα μια φορά, παρέχοντας τότε το password του, και οι συνακόλουθες αυθεντικοποιήσεις να συμβαίνουν αυτόματα. Ο προφανής τρόπος να υποστηριχθεί κάτι τέτοιο, δηλαδή αποθηκεύοντας στην cashe του σταθμού εργασίας το password του χρήστη, είναι επικίνδυνος. Μια καλύτερη προσέγγιση που χρησιμοποιεί το Kerberos, είναι να αποθηκεύει στην cashe μόνο τα εισητήρια και τα κλειδιά

κρυπτογράφησης (που όλα μαζί καλούνται credentials), που θα χρησιμοποιούνται για ένα εύλογα σύντομο χρονικό διάστημα.

Η "υπηρεσία ενοίκιασης εισητηρίων" (ticket granting service) στο πρωτόκολλο του Kerberos επιτρέπει σε έναν χρήστη να αποκτήσει εισητήρια και κλειδιά κρυπτογράφησης με τη χρήση τέτοιων credentials, χωρίς την επανα-πληκτρολόγηση του password του χρήστη. Όταν ο χρήστης πρωτο-συνδέεται, διατυπώνεται μια αίτηση αυθεντικοποίησης, και ο server αυθεντικοποίησης επιστρέφει ένα εισητήριο μαζί με ένα κλειδί επικοινωνίας για την "υπηρεσία ενοίκιασης εισητηρίων". Αυτό το εισητήριο, που καλείται **ticket granting ticket,** έχει ένα σχετικά σύντομο χρόνο ζωής (συνήθως 8 ώρες). Η απάντηση αποκρυπτογραφείται, το εισητήριο και το κλειδί επικοινωνίας αποθηκεύονται, και το password του χρήστη προς το παρόν αγνοείται.

Ακολούθως, όταν ο χρήστης επιθυμεί να αποδείξει την ταυτότητά του σε έναν καινούριο πιστοποιητή, ένα καινούριο εισητήριο αξιώνεται από τον server αυθεντικοποίησης με τη χρήση της επικοινωνία έκδοσης εισητηρίου (ticket granting exchange). Η επικοινωνία έκδοσης εισητηρίου είναι παρόμοια με την επικοινωνία αυθεντικοποίησης (authentication exchange), με εξαίρεση το γεγονός ότι η αίτηση έκδοσης εισητηρίου (ticket granting request) έχει ενσωματωμένη μέσα της μια αίτηση εφαρμογής, ενώ η απάντηση (ticket granting response) είναι κρυπτογραφημένη με το κλειδί επικοινωνίας από το ticket granting ticket, παρά με το password του χρήστη.



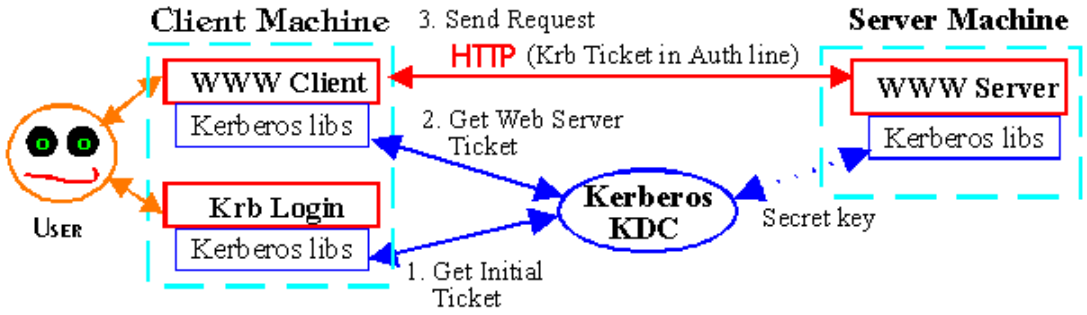
1. as_req: c, tgs, $time_{exp}$, n
2. as_rep: $\{K_{c,tgs}, tgs, time_{exp}, n, ...\}K_c$, $\{T_{c,tgs}\}K_{tgs}$
3. tgs_req: $\{ts, ...\}K_{c,tgs}$ $\{T_{c,tgs}\}K_{tgs}$, v, $time_{exp}$, n
4. tgs_rep: $\{K_{c,v}, v, time_{exp}, n, ...\}K_{c,tgs}$, $\{T_{c,v}\}K_v$
5. ap_req: $\{ts, ck, K_{subsession}, ...\}K_{c,v}$ $\{T_{c,v}\}K_v$
6. ap_rep: $\{ts\}K_{c,v}$ (optional)

Σχήμα 7

Το σχήμα δείχνει το πλήρες πρωτόκολλο αυθεντικοποίησης στο Kerberos. Τα μηνύματα 1 και 2 χρησιμοποιούνται μόνον όταν ο χρήστης πρωτο-συνδέεται στο σύστημα, τα μηνύματα 3 και 4 όταν ο χρήστης αυθεντικοποιείται σε έναν καινούριο πιστοποιητή, και το μήνυμα 5 κάθε φορά που ο χρήστης αυθεντικοποιεί τον εαυτό του (στον ίδιο πιστοποιητή). Το μήνυμα 6 είναι προαιρετικό και χρησιμοποιείται μόνον όταν ο χρήστης απαιτεί αμοιβαία αυθεντικοποίηση από τον πιστοποιητή.

2.8.1 Kerberos και Web

Με κατάλληλες προϋποθέσεις (π.χ η χρήση ενός interface όπως το GSS-API) το Kerberos μπορεί να χρησιμοποιηθεί για επικοινωνία μεταξύ servers και browsers στο Web . Έτσι, επιτυγχάνεται αμοιβαία αυθεντικοποίηση του server και του client, ο server μπορεί να ασκήσει έλεγχο προσπέλασης με βάση την αυθεντικοποίηση του client, ενώ οι αιτήσεις και οι απαντήσεις του client και του server αντίστοιχα κρυπτογραφούνται για μεγαλύτερη ασφάλεια. Το σχήμα 7 αναπαριστάνει τη διαδικασία.



Σχήμα 7 Kerberos και αυθεντικοποίηση στο Web

Firewalls 3

Ο κύριος στόχος της ύπαρξης ενός firewall είναι η προστασία ενός δικτύου από ένα άλλο δίκτυο. Το δίκτυο που προστατεύεται είναι υπό την ευθύνη ενός ή περισσοτέρων ατόμων, ενώ το δίκτυο από το οποίο προστατεύεται είναι ένα εξωτερικό δίκτυο το οποίο δεν θεωρείται έμπιστο. Έτσι, μη εξουσιοδοτημένοι χρήστες δεν έχουν πρόσβαση σε "ευαίσθητα" δεδομένα, ενώ οι νόμιμοι χρήστες διευκολύνονται στην άσκηση των κεκτημένων δικαιωμάτων τους.

Σήμερα, μπορούμε να ταξινομήσουμε τα firewalls σε δύο κατηγορίες:

1) Screening Routers ή Packet-Filtering Firewalls,
2) Application Gateways ή Proxy Firewalls,

3.1 Καταστρώνοντας μια πολιτική ασφαλείας

Προκειμένου να ασφαλίσουμε ένα ιδιωτικό δίκτυο, εγκαθιστούμε αυτό που λέγεται "περίμετρος ασφαλείας" . Η περίμετρος ασφαλείας καθορίζεται από την πολιτική ασφαλείας καθώς και από μηχανισμούς και μεθόδους που προάγουν και ενισχύουν την πολιτική αυτή. Ένα firewall μπορεί να είναι ένας από αυτούς τους μηχανισμούς ασφαλείας. Αυτό καθώς και άλλοι μηχανισμοί ασφαλείας πρέπει να εξετάζονται μετά την κατάστρωση της πολιτικής ασφαλείας που θα ακολουθηθεί, καθώς αποτελούν την υλοποίησή της. Πριν την υλοποίηση λοιπόν, θα πρέπει να έχει γίνει ανάλυση των κινδύνων και ανάλυση των απαιτήσεων.

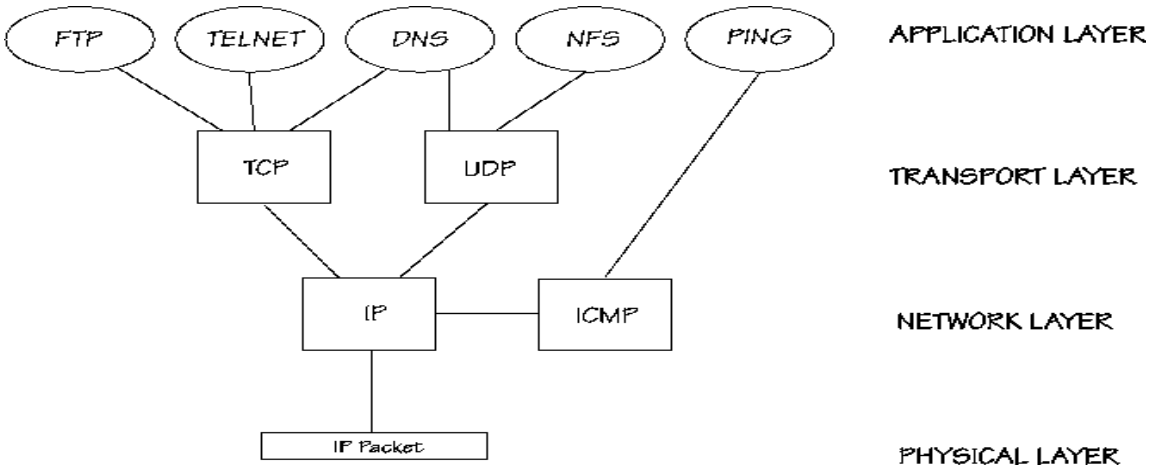
Έτσι, πρίν τεθεί το ερώτημα: *"Τί είδους Firewall πρέπει να τοποθετήσουμε στο δίκτυό μας;"* θα πρέπει να έχει απαντηθεί πλήρως το ερώτημα *"Ποιές απειλές υπάρχουν;"* Με άλλα λόγια ο οργανισμός θα πρέπει να ξέρει τί θέλει να προστατεύσει και από τί θέλει να το προστατεύσει. Στα πλαίσια της *ανάλυσης κινδύνων* λοιπόν, καθορίζονται τα τρωτά σημεία του συστήματος, οι πιθανότητες εκμετάλλευσης των τρωτών σημείων του συστήματος, τα μέτρα που πρέπει να ληφθούν σε συνάρτηση με το κόστος τους. Στη συνέχεια, και στα πλαίσια της ανάλυσης των απαιτήσεων, καθορίζονται τα χαρακτηριστικά της συγκεκριμένης υπηρεσίας που θα απαιτηθεί καθώς και τί θα συμβεί σε περίπτωση που η υπηρεσία διακοπεί.

Στη συνέχεια, και μόνον εφόσον έχει καταστρωθεί η πολιτική της εταιρίας, αποφασίζεται η επιλογή του firewall που θα πλαισιώνει τους μηχανισμούς ασφαλείας στο δίκτυο. Πρέπει να τονιστεί ότι η πολιτική ασφαλείας δεν καταστρώνεται μόνο μια φορά. Οι συνθήκες αλλάζουν συνεχώς, το Internet πέρνει καινούριες μορφές, οι αδυναμίες των συστημάτων μεταβάλλονται, τα firewalls αποκτούν καινούρια χαρακτηριστικα. Έτσι, η η πολιτική ασφαλείας πρέπει να αναθεωρείται περιοδικά, ανάλογα πάντα και με τις εξελίξεις και τις οικονομικές δυνατότητες της εταιρίας.

3.2 Screening Routers

Πολλοί εμπορικοί routers (δρομολογητές) έχουν τη δυνατότητα να "εξετάζουν" (screen) πακέτα βασισμένοι σε κριτήρια όπως ο τύπος του πρωτοκόλλου, τα πεδία διεύθυνσης πηγής (source address) και διεύθυνσης προορισμού (destination address),

καθώς και άλλα πεδία ελέγχου . Οι Screening Routers παρέχουν έναν ισχυρό μηχανισμό ελέγχου της κίνησης σε ένα δίκτυο, άρα και των υπηρεσιών που παρέχονται στο δίκτυο. Η ικανότητα του router να διαχωρίζει (να επιτρέπει ή να απορρίπτει) τα "πακέτα" με κριτήρια που αφορούν αυστηρά τις ιδιότητες του πρωτοκόλλου ονομάζεται *packet filtering* (φιλτράρισμα πακέτου).

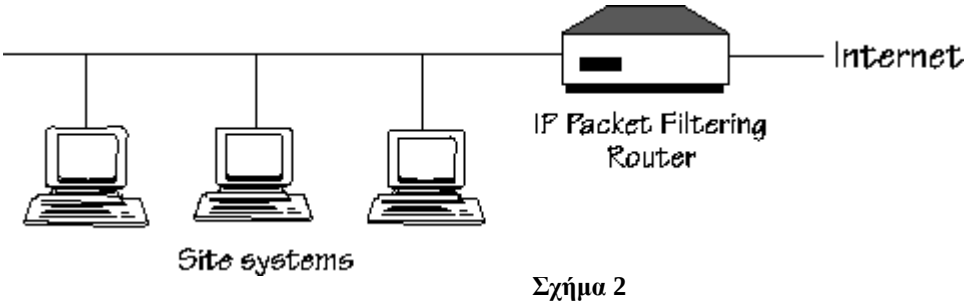


Σχήμα 1

Γενικά, η πολιτική ασφαλείας που υϊοθετείται, σκοπεύει περισσότερο στην αποτροπή των εκτός-του-δικτύου, παρά στην αστυνόμευση των εντός-του-δικτύου. Με βάση αυτό το σκεπτικό, αποφασίζεται και το σημείο στο οποίο θα τοποθετηθεί ο router, όπως και το πώς θα προγραμματστεί ώστε να επιτελεί φιλτράρισμα πακέτων. Επίσης, στόχος της πολιτικής είναι να παρέχει ένα "διάφανο" μηχανισμό, ώστε να μη γίνεται αντιληπτός στους χρήστες. Επειδή το φιλτράρισμα των πακέτων (packet filtering) πραγματοποιείται στα **επίπεδα δικτύου** (Network layer) και **μεταφοράς** (Transport layer) του μοντέλου TCP/IP, και όχι στο επίπεδο εφαρμογής, η διαφάνεια εξασφαλίζεται σε μεγάλο βαθμό.

Ένα packet filter τοποθετείται συνήθως ανάμεσα σε ένα ή περισσότερα τμήματα δικτύου (network segments) όπως φαίνεται στο σχήμα 1. Τα τμήματα δικτύου διαχωρίζονται σε εσωτερικά (internal) και σε εξωτερικά (external). Τα εξωτερικά τμήματα δικτύου συνδέουν το δίκτυο με άλλα δίκτυα όπως το Internet. Τα εσωτερικά τμήματα δικτύου συνδέουν τους hosts της επιχείρησης καθώς και άλλους πόρους εντός της επιχείρησης.

Κάθε μία από τις ports του router μπορεί να χρησιμοποιηθεί ώστε να υλοποιηθούν πολιτικές ασφαλείας που θα περιγράφουν τον τύπο της πρόσβασης δικτύου που θα επιτρέπεται διαμέσου αυτής της port. Εαν ο αριθμός των τμημάτων δικτύου που συνδέονται με τον router είναι μεγάλος, τότε οι πολιτικές που μπορούν να υλοποιθούν από τον router μπορεί να γίνουν πολύπλοκες. Επειδή η πολιτική του δικτύου καταστρώνεται ώστε να ευνοεί τους εντός-του-δικτύου όταν θέλουν να επικοινωνήσουν με εξωτερικούς hosts, το φίλτρο πρέπει να συμπεριφέρεται διαφορετικά σε κάθε πλευρά του router. Δηλαδή με άλλα λόγια, τα φίλτρα είναι **μη συμμετρικά**.



Σχήμα 2

Σχεδόν όλα τα packet-filtering firewalls λειτουργούν ως εξής:

1) Τα κριτήρια φιλτραρίσματος αποτελούν τους κανόνες φιλτραρίσματος πακέτων (packet filter rules) και μπορούν να εφαρμοστούν τόσο στην εσωτερική (ως προς το δίκτυο) όσο και στην εξωτερική (ως προς το δίκτυο) πλευρά του router.
2) Όταν ένα πακέτο φθάνει σε μια port, απομονώνονται οι επικεφαλίδες του πακέτου. Οι περισσότερες packet filter συσκευές εξετάζουν μόνο τα πεδία των IP, TCP, ή UDP πακέτων.
3) Οι κανόνες φιλτραρίσματος αποθηκεύονται με αυστηρή σειρά προτεραιότητας. Κάθε κανόνας εφαρμόζεται στο πακέτο, με τη σειρά που είναι αποθηκευμένος.
4) Εαν ένας κανόνας "μπλοκάρει" τη λήψη ή μετάδοση ενός πακέτου, το πακέτο απορρίπτεται.
5) Εαν ένας κανόνας επιτρέπει τη λήψη ή μετάδοση ενός πακέτου, το πακέτο γίνεται δεκτό.
6) Εαν ένα πακέτο δεν ικανοποιεί κανέναν κανόνα, "μπλοκάρεται".

Πλεονεκτήματα των packet filtering Firewalls

Σήμερα τα firewalls που βασίζονται στο φιλτράρισμα IP πακέτων έχουν εξελιχθεί σε αρκετά μεγάλο βαθμό, ώστε πλέον ο όρος router να αντικαθίσταται δικαιωματικά με τον όρο firewall. Υπάρχουν δύο είδη φιλτραρίσματος: το **στατικό φιλτράρισμα** και το **δυναμικό φιλτράρισμα**.

Τα **στατικά φίλτρα**, τα οποία υλοποιούνται στους routers, εξετάζουν κάθε πακέτο που φθάνει στην port και πέρνουν απόφαση δρομολόγησης βασισμένα σε πληροφορίες που υπάρχουν στην επικεφαλίδα του πακέτου (packet header), όπως διεύθυνση πηγής (source) και προορισμού (destination), πρωτόκολλα και port αριθμούς.

Τα **δυναμικά φίλτρα**, εντούτοις είναι περισσότερο "έξυπνα" και μπορούν να λάβουν αποφάσεις δρομολόγησης βασισμένα σε πρωτόκολλα υψηλότερου επιπέδου. Επίσης, και αυτό ίσως να είναι το περισσότερο σημαντικό, γνωρίζουν εαν το πακέτο είναι αναμενόμενο, με βάση την ύπαρξη προηγούμενης επικοινωνίας, δηλαδή συγκρατούν την κατάσταση του πακέτου που καταφθάνει. Έτσι, με αυτά τα φίλτρα δεν επιτρέπονται πακέτα τα οποία για παράδειγμα περιέχουν ένα διαφορετικό αριθμό SYN (Sequence Number, σε μια TCP σύνδεση) από αυτόν που αναμενόταν.

Επίσης, επειδή τα φίλτρα λειτουργούν στα επίπεδα δικτύου και μεταφοράς (TCP/IP μοντέλο), εκτός του ότι είναι διάφανα στον χρήστη, είναι εκ φύσεως περισσότερο προσαρμόσιμα σε καινούρια πρωτόκολλα.

Τα φίλτρα **δεν** απαιτούν μεγάλη επεξεργασία από την CPU, και συνήθως υλοποιούνται στο επίπεδο του λειτουργικού συστήματος. Έτσι, ιδιαίτερα σε δίκτυα υψηλής ταχύτητας (100 Megabit/second ή περισσότερο) υπάρχει μεγάλη απόδοση.

Μειονεκτήματα των packet filtering Firewalls

Οι packet filtering routers έχουν κάποιες εγγενείς αδυναμίες, οι οποίες

δημιουργούν προβλήματα στους διαχειριστές των συστημάτων:

Πρώτον, ο καθορισμός των κανόνων φιλτραρίσματος είναι μια πολύπλοκη και συχνά επίπονη διαδικασία, πόσο μάλλον όταν συνήθως δεν υπάρχουν έτοιμα προγράμματα που να τεστάρουν την αποτελεσματικότητά τους. Λάθη στην υλοποίηση του filtering κώδικα, καθιστούν τα δίκτυα τρωτά από κάθε άποψη.

Δεύτερον, η αυθεντικοποίηση του χρήστη, όπως αυτή καθορίζεται από την πολιτική ασφαλείας, υλοποιείται σε άλλα συστήματα και όχι από το firewall. Ακριβώς επειδή το firewall είναι χαμηλού-επιπέδου (ως προς το TCP/IP μοντέλο), δεν μπορεί να κατανοήσει αφηρημένες έννοιες όπως "χρήστης".

Τρίτον, οι screening routers δεν παρέχουν δυνατότητα καταγραφής (logging) των λειτουργιών που βρίσκονται σε εξέλιξη, καθιστώντας δύσκολη την ανίχνευση μιας παραβίασης. Έτσι, εαν παρακαμφθεί κάποιος κανόνας φιλτραρίσματος από κάποιον hacker, υπάρχει ο κίνδυνος να εντοπιστεί η παραβίαση αφότου ο hacker έχει ήδη επιτελέσει το έργο του.

Τέταρτον, ένας αριθμός RPC (Remote Procedure Call) υπηρεσιών είναι δύσκολο να φιλτραριστεί αποτελεσματικά, επειδή οι αντίστοιχοι servers "ακούνε" σε ports που καθορίζονται τυχαία κατά την εκκίνηση του συστήματος. Μία υπηρεσία που καλείται *portmapper* αντιστοιχεί τις αρχικές κλήσεις RPC υπηρεσιών στους προκαθορισμένους αριθμούς υπηρεσιών (δηλαδή στις ports), αλλά στους routers δεν υπάρχει τέτοια υπηρεσία. Έτσι εφόσον ο router δεν μπορεί να ξέρει σε ποιες ports "κατοικούν" οι υπηρεσίες, δεν είναι δυνατόν να μπλοκάρει αποτελεσματικά τις υπηρεσίες αυτές, εκτός και αν μπλοκάρει όλα τα UDP πακέτα (Οι RPC υπηρεσίες χρησιμοποιούν συνήθως το UDP). Μπλοκάροντας όμως το UDP σημαίνει ότι μπλοκάρονται απαραίτητες υπηρεσίες όπως το DNS (που χρησιμοποιεί το UDP).

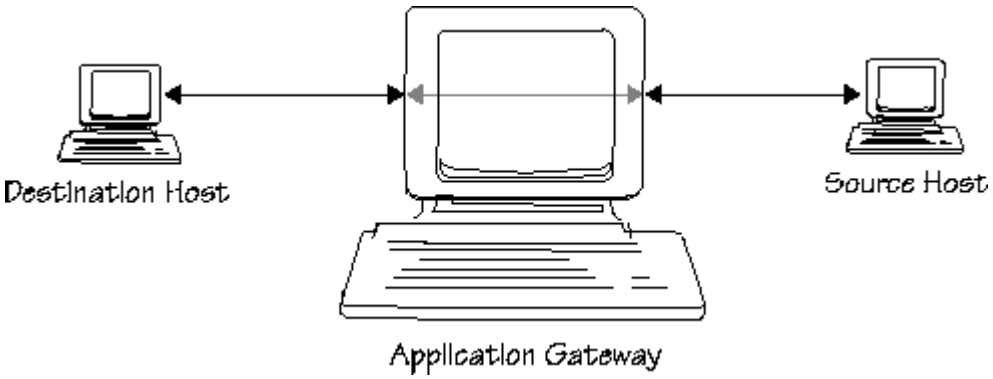
Πέμπτον, αδυναμίες των screening routers θεωρούνται και αυτές που οφείλονται στην λανθασμένη τοποθέτησή τους, όπως είδαμε και στν προηγούμενη ενότητα.

3.3 Application Gateways

Τα gateways επιπέδου εφαρμογής ή application gateways προγραμματίζονται ώστε να καταλαβαίνουν την κίνηση στο επίπεδο εφαρμογής του TCP/IP . Έτσι, παρέχουν ελέγχους προσπέλασης σε επίπεδο χρήστη και σε επίπεδο προτοκόλλων εφαρμογής.

Τα application gateways υϊοθετήθηκαν προκειμένου να εξαλειφθούν κάποιες από τις αδυναμίες που εμφανίστηκαν στην υλοποίηση των φίλτρων στους δρομολογητές **.** Έτσι, χρησιμοποιούνται software εφαρμογές, οι οποίες προωθούν και φιλτράρουν συνδέσεις για υπηρεσίες όπως HTTP, TELNET και FTP. Μια τέτοια εφαρμογή καλείται **proxy υπηρεσία**. Ένας χρήστης που επιθυμεί να συνδεθεί στο σύστημα, θα πρέπει πρώτα να συνδεθεί στο gateway και ύστερα στο host προορισμού, όπως και στο παράδειγμα που ακολουθεί (σχήμα 3):

1) Ο χρήστης κάνει telnet στο application gateway και πληκτρολογεί το όνομα ενός εσωτερικού host,
2) Το gateway ελέγχει την IP διεύθυνση του χρήστη (source) και την εγκρίνει ή την απορρίπτει, σύμφωνα με ορισμένα κριτήρια προσπέλασης,
3) Ο χρήστης ενδεχομένως να πρέπει να αυθεντικοποιήσει τον εαυτό του (π.χ χρησιμοποιώντας μια one-time password συσκευή),
4) Η proxy υπηρεσία δημιουργεί μια TELNET σύνδεση μεταξύ του gateway και του εσωτερικού host,
5) Η proxy υπηρεσία "μεταφέρει" bytes μεταξύ των δύο συνδέσεων, και
6) Το application gateway καταγράφει (log) τη σύνδεση.



Σχήμα 3 Virtual (εικονική) Σύνδεση που υλοποιείται από το application gateway και τις proxy

"Πώς δουλεύει"

Το Gateway έχει την ευθύνη να λαμβάνει πακέτα από το ένα δίκτυο και να τα παραδίδει σε ένα άλλο δίκτυο. Συνήθως αυτό σημαίνει ότι λαμβάνει πακέτα από το Internet και τα παραδίδει στο τοπικό δίκτυο (και αντιστρόφως). Το Gateway "ανοίγει" τα πακέτα, εξετάζει το περιεχόμενό τους, και εξασφαλίζει ότι δεν μπορούν να βλάψουν δυνητικά το τοπικό δίκτυο. Αφού τα πακέτα ελέγχονται ως προς την ασφάλειά τους, το Gateway "χτίζει" καινούρια, με το ίδιο περιεχόμενο. Έτσι, μόνο οι τύποι πακέτων για τους οποίους υπάρχει κώδικας κατασκευής μπορούν να εγκαταλείψουν το Gateway. Είναι αδύνατον να σταλεί μη εξουσιοδοτημένος τύπος πακέτου, αφού δεν υπάρχει κώδικας για να το δημιουργήσει. Έτσι αποτρέπονται τα "back doors". Τα καινούρια πακέτα στέλνονται μέσω ενός ξεχωριστού interface δικτύου.

Για να χρησιμοποιήσουν το Gateway, οι χρήστες πρέπει να συνδεθούν (log in) με την Gateway μηχανή, ή να υλοποιήσουν μια συγκεκριμένη client εφαρμογή σε κάθε host από τον οποίο θα συνδεθούν. Έτσι, ένα custom πρόγραμμα πρέπει να γραφτεί για κάθε εφαρμογή, και οι εφαρμογές που επιτρέπονται είναι μονάχα αυτές για τις οποίες έχει γραφτεί πρόγραμμα. Αυτό ίσως να είναι ένα εγγενές μειονέκτημα, αλλά αποτελεί πλεονέκτημα ως προς την ασφάλεια του συστήματος.

Το custom πρόγραμμα εφαρμογής λειτουργεί ως proxy που δέχεται κλήσεις και τις εξετάζει με βάση λίστες προσπέλασης που διαθέτει. Στην περίπτωση αυτή το proxy λειτουργεί ως **proxy server**. Λαμβάνοντας την κλήση και αφότου πιστοποιηθεί ότι η κλήση είναι επιτρεπόμενη, ο proxy προωθεί την αίτηση στον αντίστοιχο server. Τότε, ο proxy λειτουργεί τόσο ως server, όσο και ως client. Ως server προκειμένου να λάβει την αίτηση και ως client προκειμένου να την προωθήσει. Αφότου εγκατασταθεί η σύνδεση (session), ο proxy απλά αντιγράφει και μεταδίδει τα δεδομένα ανάμεσα στον client που έκανε την αίτηση και στον server τον οποίο στόχευε η αίτηση.

Εφόσον είναι απαραίτητη μια custom client εφαρμογή για την επικοινωνία με τον proxy server, ορισμένες standard κλήσεις συστήματος, όπως η connect( ), πρέπει να αντικατασταθούν με μια proxy έκδοση αυτών των κλήσεων συστήματος. Έπειτα, η client εφαρμογή πρέπει να μεταγλωττιστεί και να συνδεθεί με τις proxy αυτές εκδόσεις.

Πλεονεκτήματα των Application Gateways

Πλεονεκτήματα από τη χρήση των application gateways για την προστασία του συστήματος μπορούν να θεωρηθούν τα εξής:

- Τα gateways μπορούν να απορρίψουν ή να επιτρέψουν μια σύνδεση, βασιζόμενα όχι μόνο στο όνομα χρήστη, στις διευθύνσεις και τα πρωτόκολλα, αλλά προχωρούν πιο

"βαθεια": μπορούν για παράδειγμα να φιλτράρουν μια FTP σύνδεση.

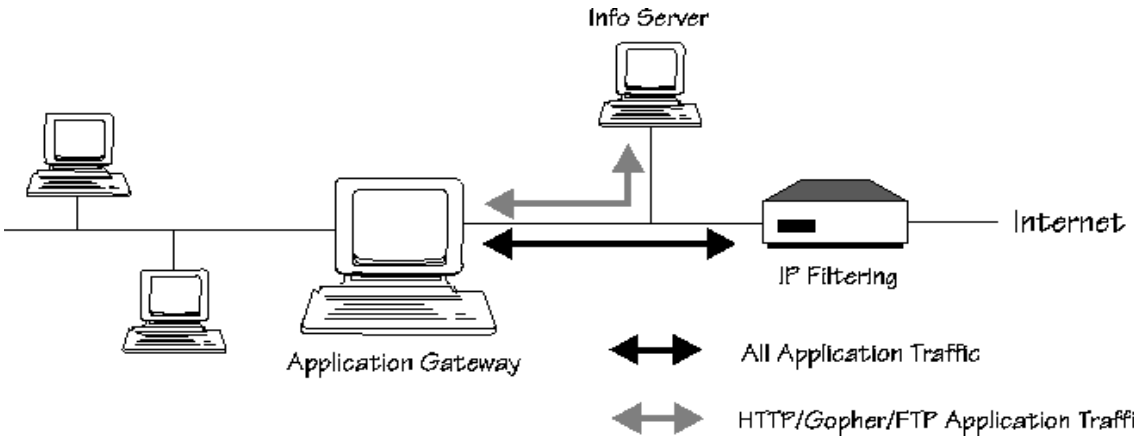
- Μπορούν να φιλτράρουν Java applets και ActiveX προγράμματα.
- Δεν επιτρέπουν την εκτέλεση εφαρμογών για τις οποίες δεν έχει γραφτεί proxy, όπως ήδη αναφέρθηκε, αυξάνοντας την ασφάλεια του συτήματος.
- Αποκρύπτουν πληροφορίες για το σύστημα, αφού τα ονόματα των εσωτερικών hosts δεν είναι απαραίτητο να είναι γνωστά μέσω DNS σε απομακρυσμένα συστήματα. Τα συστήματα αυτά χρειάζεται να γνωρίζουν μόνο το όνομα του host που "φιλοξενεί" το application gateway".
- Υποστηρίζουν τη δυνατότητα αυθεντικοποίησης (authentication) και καταγραφής (logging) .
- Είναι αποτελεσματικά ως προς το κόστος τους, καθώς το ανεξάρτητο software ή hardware που απαιτείται για την αυθεντικοποίηση ή την καταγραφή, εγκαθίσταται μόνο στο application gateway host και πουθενά αλλού.
- Σε περίπτωση που συνδυάζονται με packet filtering δρομολογητές, απαιτούν λιγότερο περίπλοκους κανόνες φιλτραρίσματος, από ότι εαν υφίστατο μονάχα ο δρομολογητής. Αυτό συμβαίνει διότι το μόνο που πρέπει να κάνει ο δρομολογητής είναι να επιτρέπει πακέτα που προορίζονται για το application gateway.

3.4 Υλοποιήσεις των Firewalls

Τα firewalls μπορούν, με συνδυασμούς από application gateways και packet filtering δρομολογητές, να υλοποιηθούν με τρείς σχηματισμούς: Dual-homed gateway, Screened host, και Screened subnet firewall.

3.4.1 Dual-homed Gateway

Στο σχήμα 4 αναπαρίσταται η διαμόρφωση ενός δικτύου υπό την προστασία ενός dual-homed host (δηλαδή ενός host που έχει δύο interfaces δικτύου). Ο host αυτός έχει απενεργοποιημένες τις λειτουργίες IP δρομολόγησης (δηλαδή, δεν μπορεί να δρομολογεί πακέτα μεταξύ των δύο δικτύων). Επιπρόσθετα, χρησιμοποιείται ένας packet filtering (screening) δρομολογητής, στο σημείο όπου συνδέεται το δίκτυο με το Internet, ώστε να υπάρχει μεγαλύτερη ασφάλεια. Έτσι, δημιουργείται ένα εσωτερικό, ελεγχόμενο (screened) subnet στο οποίο μπορούν να τοποθετηθούν ειδκά συστήματα όπως Web servers.



Σχήμα 4 Dual-homed Gateway Firewall

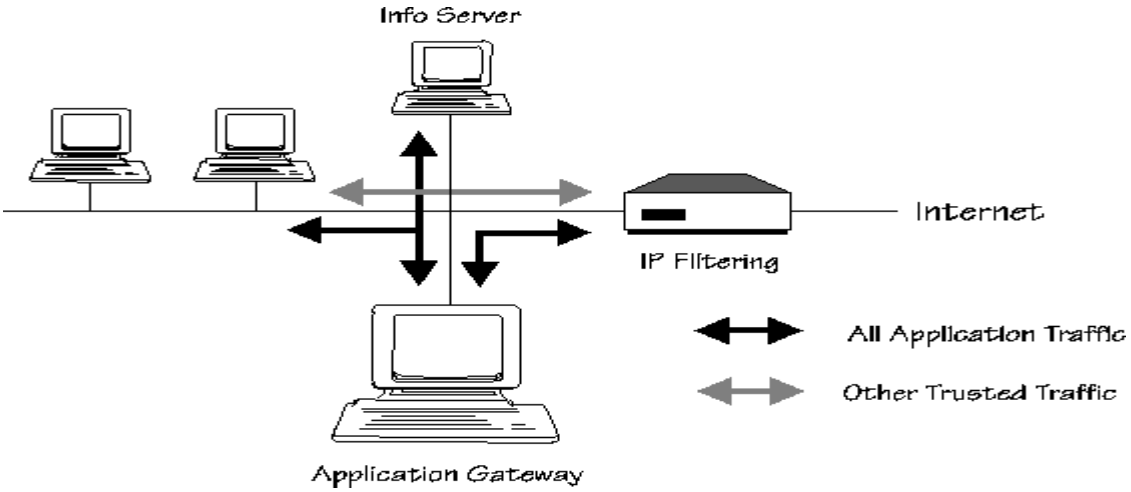
Αυτός ο τύπος firewall υλοποιεί την πολιτική ασφαλείας, σύμφωνα με την οποία "*απορρίπτεται ό,τι δεν επιτρέπεται ρητά*", εφόσον δεν υποστηρίζονται υπηρεσίες για τις

οποίες δεν υπάρχουν proxy servers στο gateway. Ο host δεν θα πρέπει να δέχεται source-routed πακέτα. (πακέτα στα οποία ο αποστολέας αναγράφει τον δρόμο που πρέπει να ακολουθήσουν, παρακάμπτοντας έτσι τους δρομολογητές). Με αυτόν το σχηματισμό εξασφαλίζεται σε μεγάλο βαθμό η ασφάλεια του δικτύου (ιδιαίτερα η ασφάλεια των hosts που βρίσκονται στο interface αριστερά του application gateway), καθώς οι "δρόμοι" προς το προστατευμένο subnet είναι γνωστοί μονάχα στο firewall και όχι στο υπόλοιπο Internet, εφόσον τα Internet συστήματα μπορούν να αποστείλουν πακέτα μονάχα στο firewall (μόνο τότε θα τα κάνει αποδεκτά ο router). Τα ονόματα και οι IP διευθύνσεις των "προστατευμένων" hosts του συστήματος είναι "κρυμμένα" από τα Internet συστήματα, εφόσον το firewall δεν χρειάζεται να μεταδίδει DNS πληροφορίες.

Εφόσον το firewall χρησιμοποιεί ένα host σύστημα, μπορεί (και πρέπει) να διαθέτει ειδικό software που θα αναγκάζει τους χρήστες να αποδείξουν την ταυτότητά τους. Οι μηχανισμοί ασφαλείας που υλοποιούνται στον host πρέπει να είναι πολύ αυστηροί και αποτελεσματικοί , καθώς το gateway είναι και το τελευταίο οχυρό ασφαλείας του συστήματος. Εαν παρακαμφθεί η ασφάλειά του, τότε ο εισβολέας μπορεί να κάνει σοβαρές παραβιάσεις. Η εγγενής ακαμψία του dual-homed gateway μπορεί να αποτελεί σοβαρό μειονέκτημα για ορισμένα sites: εφόσον οι υπηρεσίες επιτρέπονται μόνο εαν υπάρχουν proxies για αυτές, δεν μπορεί να υπάρχει πρόσβαση σε άλλες υπηρεσίες, εκτός και αν αυτές τοποθετηθούν στην Internet πλευρά του gateway (δεξιά απο το gateway στο σχήμα). Εαν δεν υπάρχει packet filtering router που να προστατεύει τις υπηρεσίες αυτές, τότε υπάρχει πρόβλημα ασφαλείας.

3.4.2 Screened Host Firewall

Το screened host (ελεγχόμενος host) firewall, που αναπαρίσταται στο σχήμα 5, παρέχει έναν πιο εύκαμπτο μηχανισμό από το dual-homed gateway firewall, αν και το τίμημα της ευκαμψίας αυτής είναι συνήθως η ασφάλεια. Ο σχηματισμός αυτός θεωρείται ιδανικός για sites που αναζητούν προστασία, αλλά όχι σε τέτοιο βαθμό ώστε να προτιμήσουν ένα dual-homed gateway.



Σχήμα 5 Screened Host Firewall

Το firewall αποτελείται από έναν packet filtering δρομολογητή και ένα application gateway, το οποίο τοποθετείται στο "προστατευμένο" subnet αριστερα από τον δρομολογητή. Το application gateway χρειάζεται μόνο ένα interface δικτύου. Οι proxy υπηρεσίες του application gateway μεταβιβάζουν FTP, TELNET, HTTP και άλλες υπηρεσίες για τις οποίες υπάρχουν proxies, στα συτήματα του site. Ο δρομολογητής φιλτράρει και ελέγχει "επικίνδυνα" πρωτόκολλα προτού αυτά φτάσουν (αν φτάσουν) στο

application gateway και στους άλλους hosts. Απορρίπτει (ή δέχεται) πακέτα εφαρμογής σύμφωνα με τους εξής κανόνες:

- Πακέτα εφαρμογής από τα Internet sites προς το application gateway, δρομολογούνται κανονικά,
- όλα τα άλλα πακέτα απορρίπτονται,
- ο δρομολογητής απορρίπτει κάθε πακέτο εφαρμογής που προέρχεται από το εσωτερικό του δικτύου, εκτός και αν έρχεται από το applicatin gateway.

Το ότι το application gateway διαθέτει μόνο ένα interface δικτύου, καθιστά το σχηματισμό περισσότερο εύκαμπτο, αλλά και λιγότερο ασφαλή, καθώς ο δρομολογητής μπορεί να παρακάμψει το gateway στην περίπτωση κάποιων "έμπιστων" υπηρεσιών. Οι έμπιστες υπηρεσίες μπορεί να είναι αυτές για τις οποίες δεν υπάρχουν proxy υπηρεσίες, και προφανώς θα είναι έμπιστες υπό την έννοια ότι η πολιτική ασφαλείας του δικτύου θα τις έχει καταστήσει έμπιστες.

3.4.3 Screened Subnet Firewall

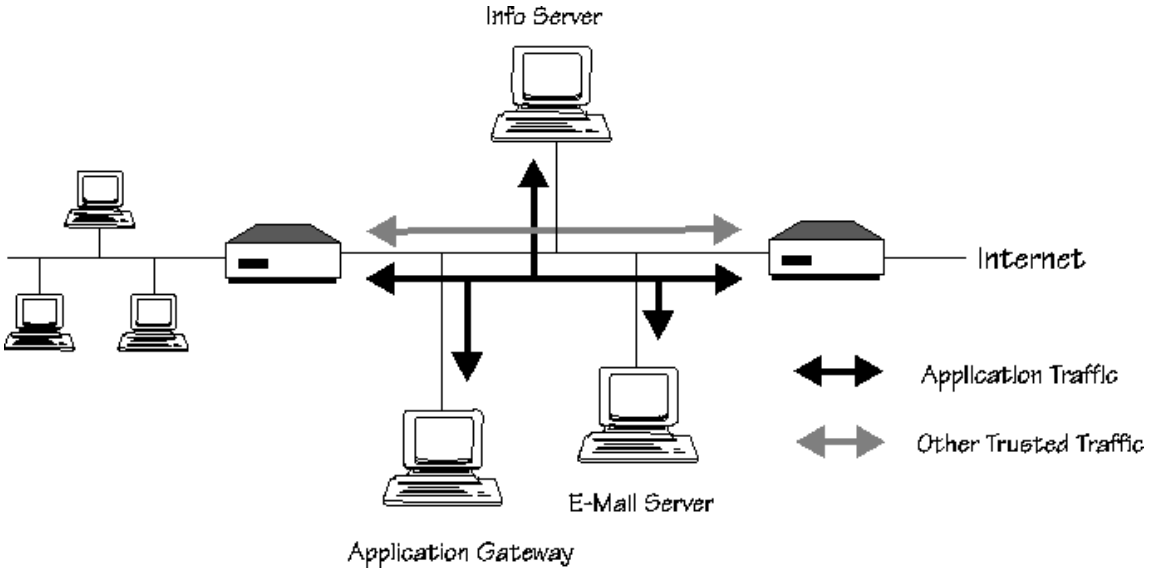
Το screened subnet (ελεγχόμενο υποδίκτυο) firewall είναι ένας συνδυασμός μεταξύ του dual-homed gateway και του screened host firewall. Στο σχήμα 6, χρησιμοποιούνται δύο δρομολογητές για τη δημιουργία ενός εσωτερικού, *ελεγχόμενου* (screened) υποδικτύου . Αυτό το subnet "φιλοξενεί" το application gateway, όπως επίσης και άλλα συστήματα που απαιτούν προσεκτικά ελεγχόμενη προσπέλαση, π.χ information servers. Ο δρομολογητής που βρίσκεται στο σημείο σύνδεσης του δικτύου με το Internet εφαρμόζει τους ακόλουθους κανόνες:

- πακέτα εφαρμογής από το application gateway στα Internet συστήματα, δρομολογούνται κανονικά,
- e-mail κίνηση από τον e-mail server προς τα Internet sites, δρομολογείται κανονικά,
- πακέτα εφαρμογής από τα Internet sites προς το application gateway, δρομολογούνται κανονικά,
- e-mail κίνηση από τα Internet sites προς τον e-mail server, δρομολογείται κανονικά,
- όλα τα άλλα πακέτα απορρίπτονται.

Ο εξωτερικός δρομολογητής επίσης, θα μπορούσε να χρησιμοποιηθεί για να "μπλοκάρει" πακέτα πρωτοκόλλων που δεν θα έπρεπε να μεταβιβάζονται προς ή από τους hosts στο screened subnet.

Ο δεύτερος δρομολογητής (εσωτερικός) δρομολογεί τα πακέτα με βάση τους ακόλουθους κανόνες:

- πακέτα εφαρμογής από το application gateway στα site συστήματα, δρομολογούνται κανονικά,
- e-mail κίνηση από τον e-mail server προς τα site συστήματα, δρομολογείται κανονικά,
- πακέτα εφαρμογής από τα site συστήματα προς το application gateway, δρομολογούνται κανονικά,
- e-mail κίνηση από τα site συστήματα προς τον e-mail server, δρομολογείται κανονικά,
- όλα τα άλλα πακέτα απορρίπτονται.



Σχήμα 6 Screened Subnet Firewall

Με το σχηματισμό αυτόν, κανένας host του δικτύου δεν είναι άμεσα προσπελάσιμος από το Internet και αντίστροφα, όπως και στο dual-homed gateway. Μια μεγάλη διαφορά όμως που υπάρχει μεταξύ των δύο μηχανισμών, είναι ότι εδώ πέρα χρησιμοποιούνται δρομολογητές προκειμένου να μεταβιβάσουν πακέτα σε ειδικά προστατευμένα συστήματα, εξαλείφοντας έτσι την ανάγκη το application gateway να έχει δύο interfaces. Το γεγονός αυτό αποτελεί και ένα μεγάλο πλεονέκτημα του σχηματισμού αυτού, καθώς είναι πιο εύκαμπτος και ενδείκνυται για δίκτυα που χρειάζονται μεγάλη ταχύτητα. Οι δύο δρομολογητές αποτελούν τα δύο βασικά "οχυρά" που πρέπει να παρακάμψει ένας hacker προκειμένου να αποκτήσει πρόσβαση στα προστατευμένα συστήματα του δικτύου.

3.5 Firewalls: Ολοένα και περισσότερο ασφαλή

Σε πολύ σύντομο χρονικό διάστημα, τα firewalls έχουν κερδίσει την εκτίμηση των περισσότερων οργανισμών στο Internet . Χωρίς αυτά, οι administrators ενός δικτύου θα έπρεπε να διατηρούν την ασφάλεια όλων των συστημάτων τους σε υψηλό επίπεδο, κάτι που είναι εξαιρετικά δύσκολο αν λάβει κανείς υπ'όψιν του το γεγονός ότι ο αριθμός των συστημάτων ανά δίκτυο αυξάνει ραγδαία στις μέρες μας.

Αυξημένες απειλές

Η σημερινή κατάσταση στο Internet εξακολουθεί να είναι πηγή ανησυχιών για τους administrators δικτύων. Ενώ πρέπει να φροντίζουν ώστε οι χρήστες να είναι "ευτυχισμένοι", με την υϊοθέτηση νέων υπηρεσιών, ταυτόχρονα πρέπει να μεριμνούν για την ασφάλειά τους. Όμως, καθώς ο αριθμός των χρηστών και των υπηρεσιών αυξάνεται κάθε μέρα, έτσι αυξάνονται και οι διαγραφόμενες απειλές.

Σήμερα υπάρχουν ειδικές ομάδες σύνταξης αναφορών περί παραβιάσεων στο Internet, οι οποίες δέχονται καθημερινά χιλιάδες κλήσεις από χρήστες που έχουν να αναφέρουν κάποια παραβίαση στο σύστημά τους. Επίσης, τα θέματα περί ασφαλείας έχουν γίνει πλέον αντικείμενο "ανοικτής" συζήτησης σε mailing lists και σε newsgroups στο USENET, όπου συζητούνται και καυτηριάζονται οι αδυναμίες των συστημάτων και οι τρόποι εκμετάλλευσής των. Έτσι, αποτρέπονται αλλά και δημιουργούνται καινούριες παραβιάσεις.

Οι source-route επιθέσεις που στοχεύουν τα συστήματα πίσω από τα firewalls,

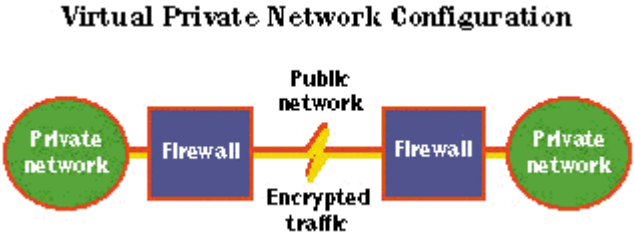
έχουν γίνει ευκολότερες χάρη στην ύπαρξη εργαλείων που αυτοματοποιούν τη διαδικασία. Επίσης, έχουν αυξηθεί οι επιθέσεις άρνησης υπηρεσίας (denial of service) οι οποίες δημιουργούν σύγχιση και ελαττώνουν την παραγωγικότητα. Συνήθεις επιθέσεις άρνησης υπηρεσίας περιλαμβάνουν το "πλημμύρισμα" (flooding) των e-mail συνδέσεων ώστε να αποτρέψουν τη χρήση τους, καθώς και την αποστολή ICMP echo πακέτων που κορέζουν τα δίκτυα μπλοκάροντας τις επικοινωνίες. Ορισμένα firewalls παραμένουν ευάλωτα σε αυτού του είδους τις επιθέσεις.

Καινούρια χαρακτηριστικά

Αποκρινόμενοι στις αυξανόμενες απειλές, οι εταιρίες firewalls έχουν εισάγει αρκετά καινούρια χαρακτηριστικά στα προϊόντα τους. Αυτά τα χαρακτηριστικά ποικίλουν από την αύξηση των τύπων των proxies και των υπηρεσιών που υποστηρίζουν, εως την αύξηση των μηχανισμών ασφαλείας και της ευκολίας διαχείρισης:

- ***Εργαλεία Διαχείρισης και Διαμόρφωσης των firewalls*** εμφανίζονται καθημερινά στην αγορά του Internet. Ορισμένα firewalls χρησιμοποιούν GUIs (Graphical User Interfaces) ώστε να διευκολύνονται οι administrators στην διαμόρφωσή τους. Άλλα συστήματα firewalls επιτρέπουν την απομακρυσμένη άσκηση διαχείρισης και ελέγχου ορθότητας (auditing) μέσω διαφόρων πρωτοκόλλων, όπως το SMTP (Simple mail Transfer Protocol), το SNMP (Simple Network Management Protocol) και το HTTP μέσω του World Wide Web. Εξυπακούεται ότι αυτοί οι μηχανισμοί προϋποθέτουν ισχυρή αυθεντικοποίηση και ελέγχους προσπέλασης.

- ***Virtual Private Networks*** (Εικονικά Ιδιωτικά Δίκτυα)**:** Σε πολλές επιχειρήσεις υπάρχει η ανάγκη ασφαλούς επικοινωνίας μεταξύ των ιδιωτικών δικτύων που διαθέτουν σε διαφορετικά σημεία στο Internet. Προκειμένου να εξασφαλίσουν την ασφάλεια τέτοιου είδους επικοινωνιών, οι εταιρίες firewalls εφαρμόζουν κρυπτογραφικούς μηχανισμούς στα προϊόντα τους με σκοπό τη δημιουργία ενός virtual ιδιωτικού δικτύου μεταξύ δύο sites, όπου η πληροφορία μεταδίδεται κρυπτογραφημένη. Τα VPNs επιτυγχάνονται με κρυπτογράφιση στο επίπεδο του Internet Protocol, μεταξύ δύο "συνεργαζόμενων" firewalls. Εφόσον το VPN εγκατασταθεί, οι hosts σε ένα σημείο μπορούν να επικοινωνούν με τους hosts στο απομακρυσμένο σημείο χωρίς το φόβο της παραβίασης της εμπιστευτικότητας των πληροφοριών που ανταλάσσονται. Φυσικά, όπως και σε κάθε κρυπτογραφικό σχήμα, το VPN είναι ασφαλές εφόσον είναι ασφαλή και τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται.



- ***Network Address Translation***: Σε μια διαδικασία NAT (Μετάφραση Διεύθυνσης Δικτύου), το firewall αντικαθιστά τις IP διευθύνσεις των πακέτων με διαφορετικές διευθύνσεις. Αυτό μπορεί να γίνει για διάφορους λόγους, οι περισσότεροι από τους οποίους σχετίζονται με την ασφάλεια. Καταρχήν, το NAT επιτρέπει σε έναν οργανισμό να αποκρύψει τόσο την ύπαρξη συγκεκριμένων συστημάτων στο

εσωτερικό του δίκτυο, όπως και την δομή καθ'αυτή του εσωτερικού του δικτύου. Ένα χαρακτηριστικό που καθιστά το NAT πολύ ελκυστικό αλλά δεν σχετίζεται με την ασφάλεια, είναι η ικανότητά του να μετατρέπει hosts δικτύου με μη μοναδικές διευθύνσεις, σε hosts με μοναδικές διευθύνσεις, επιτρέποντας έτσι στον οργανισμό να συνδεθεί με το Internet.

Αυτή η τεχνική είναι χρήσιμη στο να "κρύβει" διευθύνσεις που περιέχονται σε επικεφαλίδες πακέτων. Εντούτοις, προκειμένου να αποκρύπτονται αποτελεσματικά οι εσωτερικές διευθύνσεις, είναι προτιμότερη η "παρέμβαση" μέσα στο πακέτο καθ'αυτό. Έτσι, ορισμένα προϊόντα firewalls ξαναγράφουν π.χ τις e-mail επικεφαλίδες ώστε να κρύψουν το όνομα του εσωτερικού συστήματος από το οποίο προήλθε το μήνυμα.

- ***Καινούρια proxies και υπηρεσίες***: Με στόχο την επέκταση της λειτουργικότητας των firewalls, ολοένα και περισσότερα proxies προστίθενται στα συστήματα. Αυτό είναι και ένα από τα χαρακτηριστικά στο οποίο "ποντάρουν" οι πωλητές firewalls. Ούτως ή άλλως, εαν δεν υπάρχουν διαθέσιμα τα κατάλληλα proxies, οι υπηρεσίες προς τους πελάτες και τους χρήστες ελαττώνονται αισθητά, ενώ αυξάνεται και ο φόρτος των administrators που πρέπει να παρακάμπτουν τα firewalls διατηρώντας παράλληλα το σύστημα ασφαλές.

- ***Transparent Proxies*** (Διάφανα Proxies): Εκτός από τα proxies που αναφέρθηκαν προηγουμένως, οι πωλητές firewalls υλοποιούν επίσης τα λεγόμενα *διαφανα proxies*. *Διάφανο proxy* υφίσταται όταν οι χρήστες δεν ξέρουν ότι όντως χρησιμοποιείται ένα proxy. Οι χρήστες, μπορούν να είναι ενήμεροι για την ύπαρξη ενός proxy, με δύο τρόπους: πρώτον, μερικά proxies απαιτούν αλληλεπίδραση του χρήστη με το firewall, όπως π.χ η πληκτρολόγηση ενός ID και ενός συνθηματικού. Δεύτερον, ένα μη-διάφανο proxy μπορεί να απαιτεί την εγκατάσταση custom client software από τον χρήστη, όπως π.χ οι clients που βασίζονται στο Socks. Πολλοί οργανισμοί θα προτιμούσαν να μην επιφορτώνουν τους χρήστες τους με τέτοιες διαδικασίες, κάτι που εξασφαλίζεται με τα *διάφανα proxies.* Εντούτοις, τα *διάφανα proxies* απαιτούν μερικές ρυθμίσεις σε ορισμένα client sotware.

- ***Καταγραφή (log) και έλεγχος ορθότητας***: Τα περισσότερα firewalls παρέχουν μηχανισμούς καταγραφής (logging) λειτουργιών. Εντούτοις, ορισμένα firewalls παρέχουν τη δυνατότητα υποστήριξης μηχανισμών ελέγχου ορθότητας (audit) και προειδοποιητικών (alert) μηχανισμών. Τα auditing εργαλεία επεξεργάζονται την ήδη καταγραφόμενη (από τα logs) πληροφορία και την παρουσιάζουν με έναν περισσότερο ευανάγνωστο τρόπο. Οι alert μηχανισμοί πληροφορούν σε πραγματικό χρόνο τους administrators για "επικίνδυνες" λειτουργίες που επιχειρούνται στο firewall. Επιπρόσθετα, το SNMP μπορεί να χρησιμοποιηθεί για την προειδοποίηση (alert) απομακρυσμένων hosts.

3.6 Κριτήρια επιλογής ενός firewall

Ίσως η σημαντικότερη απόφαση που πρέπει να πάρει ένας οργανισμός που επιδιώκει να εγκαταστήσει ένα ασφαλές δίκτυο στο Internet, είναι η επιλογή του κατάλληλου firewall που θα πλαισιώσει τους μηχανισμούς ασφαλείας του δικτύου. Τα κριτήρια επιλογής ενός firewall, εξαρτώνται άμεσα από τα ακόλουθα θέματα:

Λειτουργικό σύστημα (OS)

Μέχρι πρότινος, το λειτουργικό σύστημα που επιλέγονταν από τους περισσότερους οργανισμούς ήταν το UNIX, έχοντας Ethernet για LAN interface. Στην πραγματικότητα, υπάρχουν προϊόντα που δουλεύουν σε συγκεκριμένες εκδόσεις του UNIX, για συγκεκριμένο hardware. Καθώς όμως τα Windows NT γίνονται ολοένα και περισσότερο δημοφιλή, αρχίζει να υπάρχει αυξημένη ζήτηση στο Internet για Windows NT firewalls. Πολλές εταιρίες των οποίων τα προϊόντα έχουν κερδίσει την εμπιστοσύνη αρκετών στο διαδίκτυο, έχουν ανακοινώσει την πρώτη "φουρνιά" firewalls για το δημοφιλές λειτουργικό.

Μερικοί πιστεύουν ότι τα Windows NT δεν είναι τόσο ασφαλή όσο το UNIX. Άλλοι πιστεύουν το αντίθετο. Ένα αρνητικό σημείο στη χρήση των Windows NT είναι ίσως το γεγονός ότι, όταν υπάρχει κάποιο πρόβλημα, πρέπει να αναλάβει η Microsoft τη διόρθωσή του. Αντίθετα με το UNIX, όπου η ιδιωτική πρωτοβουλία έχει πάντα θετικά αποτελέσματα.

Η επιλογή της πλατφόρμας, πάνω στην οποία θα "τρέχει" το firewall, εξαρτάται εν τέλει από τη φύση του δικτύου και από το κατά πόσο οι administrators αισθάνονται "άνετα" με το ένα ή το άλλο λειτουργικό.

Αρχιτεκτονική

Η αρχιτεκτονική ενός firewall περιλαμβάνει τις εγγενείς δυνατότητές του καθώς και διάφορους ειδικούς μηχανισμούς που ενσωματώνει προκειμένου να ενισχύσει την ασφάλεια που παρέχει. Ένα firewall πρέπει καταρχήν να είναι "χτισμένο" επάνω σε ασφαλές OS, και να επιτρέπει την έλευση μόνο σε συγκεκριμένους τύπους πακέτων.
Η ειρωνία είναι, ότι όσο περισσότερα πρωτόκολλα και υπηρεσίες υποστηρίζει ένα firewall, τόσο μεγαλύτερη είναι η πιθανότητα παράκαμψής του από κάποιον επιτήδειο. Τα περισσότερα firewalls υποστηρίζουν τις δημοφιλείς IP υπηρεσίες, ,αλλά διαφέρουν στον τρόπο με τον οποίο υλοποιούν αυτήν την υποστήριξη.

Όταν πιστοποιούν την ακεραιότητα των συστημάτων τους, ορισμένα firewalls ελέγχουν ψηφιακές υπογραφές, είτε στον κώδικα των προγραμμάτων που λειτουργούν, είτε σε αρχεία συστήματος. Ο τρόπος με τον οποίο αντιδρούν τα firewalls σε μια διαπιστωμένη παραβίαση, διαφέρει δραματικά από firewall σε firewall.

Διαχείριση (Configuration)

Λέγοντας διαχείριση εννοούμε το περιβάλλον κάτω από το οποίο ο χρήστης του firewall (ο administrator) ενεργοποιεί ή απενεργοποιεί πρωτόκολλα, περιορίζει τις παρεχόμενες υπηρεσίες με κριτήριο ονόματα χρηστών ή/και διευθύνσεις, πιστοποιεί και ελέγχει τις παραμέτρους του συστήματος. Ιδανικά, ένα firewall πρέπει να παρέχει στους διαχειριστές των δικτύων ένα ξεκάθαρο σύνολο επιλογών και ρυθμίσεων για κάθε πρωτόκολλο, και μια ευέλικτη μέθοδο ελέγχου των τρεχουσών ρυθμίσεων. Εαν οι διαχειριστές δεν μπορούν εύκολα να καθορίζουν τα πρωτόκολλα που "ελέγχονται" και να αλλάζουν τις ρυθμίσεις, τότε το firewall μάλλον δυσχεραίνει παρά διευκολύνει τις προσπάθειές τους. Έτσι, τα firewalls που διαθέτουν GUIs (Graphical User Interfaces) έχουν το προβάδισμα σε αυτόν τον τομέα.

Σύστημα προειδοποίησης

Ένα "ισχυρό" σύστημα προειδοποίησης σε ένα firewall θα πρέπει να περιλαμβάνει ενημέρωση σχετικά με το τρέχων status λειτουργίας, λάθη που έχουν γίνει, πιθανές ενέργειες παραβιάσεων, και "συναγερμούς" προειδοποίησης. Το ιδανικό firewall θα πρέπει έγκαιρα και σε πραγματικό χρόνο να ενημερώνει το διαχειριστή για οποιοδήποτε πρόβλημα.

Αυθεντικοποίηση

Ένα αξιόπιστο firewall θα πρέπει να διαθέτει ισχυρούς μηχανισμούς αυθεντικοποίησης, για όσους συνδέονται σε αυτό ή διαμέσου αυτού. Σήμερα, τα firewalls χρησιμοποιούν one-time passwords, ψηφιακές υπογραφές πακέτων, και επαναχρησιμοποιήσιμα passwords.

Τα one-time passwords είναι έγκυρα για μία και μόνο σύνδεση. Εαν συνδυάζονται και με ψηφιακές υπογραφές, αποτελούν ισχυρό όπλο στα χέρια των administrators.

Οι υπογραφές πακέτων είναι προσδιοριστές αυθεντικοποίησης (authentication indicators) που περιλαμβάνονται σε ένα πακέτο δεδομένων (συνήθως σε όλα τα πακέτα μιας σύνδεσης) και που χρησιμοποιούν κρυπτογράφηση δημοσίου-/ιδιωτικού κλειδιού για τη ψηφιακή υπογραφή κάθε πακέτου. Τα επαναχρησιμοποιήσιμα passwords παραμένουν απαράλλαχτα για πολλαπλές login συνδέσεις. Δεν είναι ασφαλή και αποτελούν την έσχατη λύση. Η πιο ασφαλής λύση αυθεντικοποίησης συνδυάζει τα one-time passwords με τις ψηφιακές υπογραφές πακέτων.

Κρυπτογραφία

Υπάρχουν τρεις μέθοδοι κρυπτογράφησης. Τα δεδομένα μπορεί να κρυπτογραφούνται και να αποκρυπτογραφούνται μεταξύ δύο firewalls, μεταξύ δύο standalone servers που βρίσκονται πίσω από firewalls, και τέλος μεταξύ ενός firewall και ενός απομακρυσμένου PC. Ιδανικά, κάθε πωλητής firewall θα πρέπει να παρέχει standalone PC software που θα επιτρέπει στους "μη στάσιμους" χρήστες να συνδέονται (από οπουδήποτε στον κόσμο) με το firewall μέσω ενός κρυπτογραφημένου καναλιού επικοινωνίας στο Internet.

Η κρυπτογραφία αποτελεί σημαντικό και χρήσιμο κομμάτι της απομακρυσμένης διαχείρισης ενός firewall, καθώς passwords και άλλες ευαίσθητες πληροφορίες που διακινούνται μεταξύ του απομακρυσμένου σταθμού εργασίας του διαχειριστή και του firewall, "εκτίθενται" στο Internet. Με δεδομένο ότι τα "παραδοσιακά" πρωτόκολλα όπως το telnet και το SNMP δεν προβλέπουν κρυπτογράφηση των δεδομένων, είναι πολύ σημαντικό για ένα firewall να παρέχει ένα ασφαλές κανάλι επικοινωνίας.

Όπως και σε κάθε κρυπτογραφικό σχήμα, έτσι και στην περίπτωση των firewalls η ασφάλεια του κρυπτογραφήματος εξαρτάται από το κλειδί κρυπτογράφισης . Το ερώτημα που τίθεται είναι "πόσο μεγάλο πρέπει να είναι το κλειδί;" Τα πιο κοινά σχήματα χρησιμοποιούν κλειδιά των 56bits και των 128 bits.

Επίσης, το "πού" γίνεται η κρυπτογράφηση παίζει σημαντικό ρόλο. Μερικά προϊόντα firewalls κρυπτογραφούν ολόκληρο το IP πακέτο, συμπεριλαμβανομένης και της επικεφαλίδας (header), ουσιαστικά ενθυλακώνοντάς το σε ένα δεύτερο IP πακέτο.

Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιείται στα firewalls, έχει γίνει πολλές φορές στο παρελθόν αντικείμενο συζήτησης. Ένα από τα συστήματα που χρησιμοποιείται κατα κόρον είναι το δημοφιλές DES (Data Encryption Standard). Κρυπτογραφεί ανά 64-bit blocks κειμένου με τη χρήση ενός κλειδιού 56 bits, έχοντας ως αποτέλεσμα τρισεκκατομύρια πιθανών μεταθέσεων του κειμένου. Αυτό ίσως να ακούγεται εντυπωσιακό, αλλά με την υπάρχουσα τεχνολογία, ένα πολύ ισχυρό workstation μπορεί να "σπάσει" το κρυπτογράφημα. Έτσι, αρκετοί πιστεύουν ότι το DES θα "πεθάνει" σε μερικά χρόνια. Εντούτοις, μια επέκταση του συστήματος DES, το triple DES (τριπλό DES), αρχίζει να ξεπροβάλλει ως το de facto εμπορικό standard. Αυτό το σχήμα κρυπτογραφεί κάθε block κειμένου τρεις φορές, χρησιμοποιώντας τρία διαφορετικά κλειδιά.

Κάποια firewalls χρησιμοποιούν συστήματα δημόσιου κλειδιού, ενώ κάποια προτιμούν την κρυπτογράφηση με ιδιωτικό κλειδί. Στη δεύτερη περίπτωση, αυτό που παρουσιάζει ενδιαφέρον είναι οι μηχανισμοί διαχείρισης και διανομής κλειδιών που επιλέγονται σε κάθε περίπτωση. Οι administrators έχουν να επιλέξουν μεταξύ τριων μεθόδων διανομής κλειδιών: με mail, μέσω τηλεφώνου, ή τέλος "στήνοντας" έναν server που θα αναλαμβάνει την διανομή με ασφαλή τρόπο. Αυτή είναι η προσέγγιση που υλοποιείται στο σύστημα Kerberos, το περίφημο σύστημα ασφαλείας που αναπτύχθηκε από την MIT (Massachusetts Institute of Technology). Το σύστημα Kerberos χρησιμοποιείται και στα συστήματα δημοσίου κλειδιού, για την διανομή του μυστικού κλειδιού.

Τα κρυπτογραφικά σχήματα που ενσωματώνονται στα firewalls, ειδικά αυτά που υϊοθετούν συστήματα δημοσίου κλειδιού, έχουν και το τίμημά τους. Ελαττώνουν την απόδοση του συστήματος που "κουβαλάει" το firewall. Η κρυπτογράφηση απασχολεί σε μεγάλο βαθμό την κεντρική μονάδα επεξεργασίας ενός υπολογιστή (CPU) καθυστερώντας την επεξεργασία των IP πακέτων. Έτσι, ορισμένες εταιρίες ενσωματώνουν encryption chips στα προϊόντα τους, ώστε να απαλάσσουν τη CPU από επιπλέον φόρτο.

Ασφάλεια και Java 4

4.1 Λειτουργικότητα της Java.

Η γλώσσα Java άλλαξε τη μέχρι πρότινος "παθητική" φύση του World Wide Web, εισάγοντας την έννοια του "αρχιτεκτονικά ουδέτερου" κώδικα που φορτώνεται δυναμικά και εκτελείται σε ένα ετερογενές δίκτυο μηχανών, όπως το Internet. Η λειτουργικότητα της γλώσσας οφείλεται στην αντικειμενοστρεφή δομή της, το "αυστηρό" περιβάλλον της, την multithreading δυνατότητά της, την ευκολία χρήσης της. Κατανοώντας την αρχιτεκτονική του περιβάλλοντος της Java και τον τρόπο με τον οποίο αυτή σχετίζεται με την ασφάλεια, θα είναι το πρώτο βήμα προκειμένου να συνηδειτοποιήσουμε τη "δυναμική" της γλώσσας και τη συμβολή της στον κόσμο των υπολογιστικών συστημάτων. Η λειτουργικότητα της Java συνίσταται στην ενσωμάτωση των ακόλουθων χαρακτηριστικών στην αρχιτεκτονική της:

- **Είναι μεταφέρσιμη.** Η Java μπορεί να τρέξει σε οποιονδήποτε υπολογιστή που διαθέτει Java interpreter. Αυτό σημαίνει ότι κάθε computer που θέλει να "τρέξει" Java, θα πρέπει να διαθέτει ένα πρόγραμμα που θα μετατρέψει τον Java κώδικα σε γλώσσα μηχανής. Εκτελούμενος σε interpreter περιβάλλον, ο Java κώδικας δεν χρειάζεται να προσαρμοστεί σε συγκεκριμένη hardware πλατφόρμα. Ο Java compiler που δημιουργεί τα εκτελέσιμα προγράμματα από πηγαίο κώδικα, μεταγλωττίζει για μια μηχανή που ουσιαστικά δεν υπάρχει.-η Java Virtual Machine (JVM). Η JVM είναι ένας υποθετικός επεξεργαστής που μπορεί να τρέξει Java κώδικα.

Το παραδοσιακό πρόβλημα με τους interpreters, ήταν πάντα η έλλειψη ταχύτητας. Η Java επιχειρεί να ξεπεράσει αυτό το πρόβλημα, μεταγλωττίζοντας σε ένα ενδιάμεσο στάδιο και μετατρέποντας τον Java κώδικα σε bytecode, ο οποίος έπειτα μετατρέπεται σε γλώσσα μηχανής για συγκεκριμένο επεξεργαστή.

- **Είναι "αυστηρή".** Οι δημιουργοί της Java, αρχικά επιχείρησαν να επεκτείνουν την C++, αλλά γρήγορα διαπίστωσαν ότι κάτι τέτοιο θα δημιουργούσε προβλήματα. Τα μεγαλύτερα εμπόδια του να καταστεί η C++ μεταφέρσιμη, ήταν η χρήση δεικτών για απευθείας διευθυνσιοδότηση της μνήμης, και η έλλειψη αυτόματης διαχείρισης της μνήμης. Αντίθετα, η Java δεν χρησιμοποιεί pointers και παρέχει αυτόματη διαχείριση μνήμης.

Η Java παρέχει αυτόματη διαχείριση μνήμης υπό τη μορφή "Αυτόματου συλλέκτη σκουπιδιών" (Automatic garbage collector). Ο garbage collector παρακολουθεί όλα τα αντικείμενα και τις αναφορές στα αντικείμενα, σε ένα πρόγραμμα Java. Όταν δεν υπάρχει αναφορά σε ένα αντικείμενο, ο garbage collector το "σταμπάρει" προορίζοντας το για απαλλαγή. Ο collector εκτελεί ένα thread (νήμα) χαμηλής προτεραιότητας στο background και "απαλλάσει" το αντικείμενο, ελευθερώνοντας μνήμη, είτε όταν το πρόγραμμα δεν χρησιμοποιεί πολλούς κύκλους επεξεργαστή, ή όταν υπάρχει ανάγκη για περισσότερη μνήμη. Εκτελώντας ένα ξεχωριστό thread, ο garbage collector παρέχει την ευκολία χρήσης και την αυστηρότητα ενός συστήματος αυτόματης διαχείρισης μνήμης, εξαλείφοντας το υπερφόρτωμα (overhead) που θα δημιουργούσε ένα full-time σχήμα διαχείρισης μνήμης.

- **Είναι ασφαλής.** Η Java παρέχει ασφάλεια χάρη στα εξής χαρακτηριστικά του runtime περιβάλλοντός της, που θα αναλυθούν στη συνέχεια:

  -Bytecode verifier (πιστοποιητής bytecode)
  -Runtime memory layout (runtime διάταξη μνήμης)
  -Security manager (Διαχειριστής ασφαλείας)

- **Είναι αντικειμενοστρεφής.** Έτσι, εξασφαλίζεται η επαναχρησιμοποίηση του κώδικα, η επεκτασιμότητά του και οι δυναμικές εφαρμογές που δημιουργούνται με αυτόν.

Η Τάξη (Class) είναι μια συλλογή μεταβλητών και μεθόδων που ενθυλακώνει λειτουργικότητα σε ένα επαναχρησιμοποιήσιμο και δυναμικό αντικείμενο. Έτσι, αφότου δημιουργηθεί η Τάξη, μπορεί να χρησιμοποιηθεί ως template για τη δημιουργία επιπρόσθετων Τάξεων που παρέχουν επιπλέον λειτουργικότητα. Ένας προγραμματιστής για παράδειγμα, μπορεί να δημιουργήσει μια Τάξη για την εμφάνιση τετραγώνων στην οθόνη, και έπειτα να αποφασίσει ότι θα ήθελε να εμφανίζονται χρωματιστά τετράγωνα. Αντί να κατασκευάσει μια καινούρια Τάξη, ο προγραμματσιστής μπορεί απλά να αναθέσει στην Java να χρησιμοποιήσει την παλιά Τάξη, με κάποια επιπλέον χαρακτηριστικά. Ουσιαστικά, ο χρήστης μπορεί να έχει το ίδιο αποτέλεσμα χωρίς να διαθέτει τον αρχικό πηγαίο κώδικα.

Αφότου δημιουργηθεί μια Τάξη, το Java runtime περιβάλλον επιτρέπει το δυναμικό "φόρτωμα" Τάξεων. Αυτό σημαίνει ότι ήδη υπάρχουσες εφαρμογές μπορούν να αποκτήσουν περισσότερη λειτουργικότητα συνδεόμενες με Τάξεις που εμπεριέχουν τις απαραίτητες μεθόδους. Έτσι για παράδειγμα, ένας χρήστης που πλοηγείται στο Web βρίσκει ένα αρχείο για το οποίο δεν διαθέτει helper εφαρμογή. Χωρίς Java, ο χρήστης θα "κολλούσε" ψάχνωντας μια εφαρμογή που θα χειρίζονταν το αρχείο. Με Java, ο browser ζητάει από τον server μια Τάξη που μπορεί να χειριστεί το αρχείο, την "φορτώνει" δυναμικά μαζί με το αρχείο και το εμφανίζει χωρίς επιπλέον καθυστέρηση.

- **Είναι υψηλής απόδοσης.** Συνήθως το τίμημα της μεταφερσιμότητας, της ασφάλειας και της "αυστηρότητας", είναι η χαμηλή απόδοση. Είναι δύσκολο να πιστέψει κανείς ότι ο interpreted κώδικας μπορεί να "τρέχει" το ίδιο γρήγορα με τον κώδικα μηχανής. Η Java, πάραυτα, χρησιμοποιεί ορισμένα tricks (κόλπα), που μειώνουν αρκετά το φόρτο λειτουργίας:

- **multithreading δυνατότητες.** Σπάνια ένα πρόγραμα χρησιμοποιεί συνεχώς την CPU. Συνήθως τα προγράμματα αναμένουν για input χρήστη, πρόσβαση αρχείου ή δικτύου.Έτσι ο επεξεργαστής μένει αχρησιμοποίητος σε single-threaded εφαρμογές. Αντίθετα, η Java χρησιμοποιεί το idle αυτό χρονικό διάστημα για το καθάρισμα από "σκουπίδια" και για γενική συντήρηση του συστήματος.

- **Αποτελεσματικά bytecodes.** Επιπλέον, τα μεταγλωττισμένα Java bytecodes μοιάζουν πάρα πολύ με κώδικα μηχανής, οπότε η μετάφρασή τους (interpreting) σε κάποια συγκεκριμένη πλατφόρμα είναι πολύ αποτελεσματική.

Ο πρώτος Java Web Server

Στις αρχές του Αυγούστου 1997, η Sun Microsystems Inc. ανακοίνωσε τον πρώτο Java Web Server, ο οποίος εκμεταλλεύεται τη λειτουργικότητα της γλώσσας Java στο έπακρον. Ο νεωτερισμός που προκύπτει από αυτήν την πρωτοβουλία είναι η Java-κεντρική προσέγγιση στη δομή του server. Εκτελώντας Java applets στο εσωτερικό του server αντί στον client συνιστά μια υπέρβαση της μέχρι πρότινος φιλοσοφίας των World Wide Web servers, μεταφέροντας όλα τα client προνόμια στην server "πλευρά" του Web.

Η δυνατότητα διαχείρισης ενός Web server με τεχνολογίες εγγενείς στον Web – ένας browser και HTML είναι ένα σημαντικό χαρακτηριστικό διότι επιτρέπει στους administrators να διαχειρίζονται τον Web server από οποιονδήποτε TCP/IP υπολογιστή στο Internet. Βέβαια, το τίμημα συχνά είναι ακριβό: η πρόσβαση σε real-time στατιστικά όπως η χρησιμοποίηση της CPU σημαίνει ότι η HTML σελίδα πρέπει να ανανεώνεται (refresh) συχνά.

Ο Java Web Server παρέχει ένα interface Web διαχείρισης, στο οποίο εμφανίζονται real-time πληροφορίες ανεξαρτήτως πλατφόρμας (OS), μέσω της Java. Ο administrator, δουλεύοντας στο εκτελούμενο Java applet μπορεί να τελέσει τις συνήθεις εργασίες διαχείρισης, όπως εγκατάσταση των virtual servers και των καταλόγων (directories), δημιουργία Λιστών Ελέγχου Πρόσβασης (Access Control Lists), καθορισμός παραμέτρων ταχύτητας-απόδοσης.

4.2 Μηχανισμοί ασφαλείας της Java.

Η εκτέλεση του κώδικα που έχει μεταγλωττιστεί για την JVM, εναπόκειται στον interpreter. Η διαδικασία μπορεί να διαιρεθεί σε τρείς υπο-διαδικασίες :

-Φόρτωμα του κώδικα
-Πιστοποίηση
-Εκτέλεση.

Η Γλώσσα και ο Μεταγλωττιστής

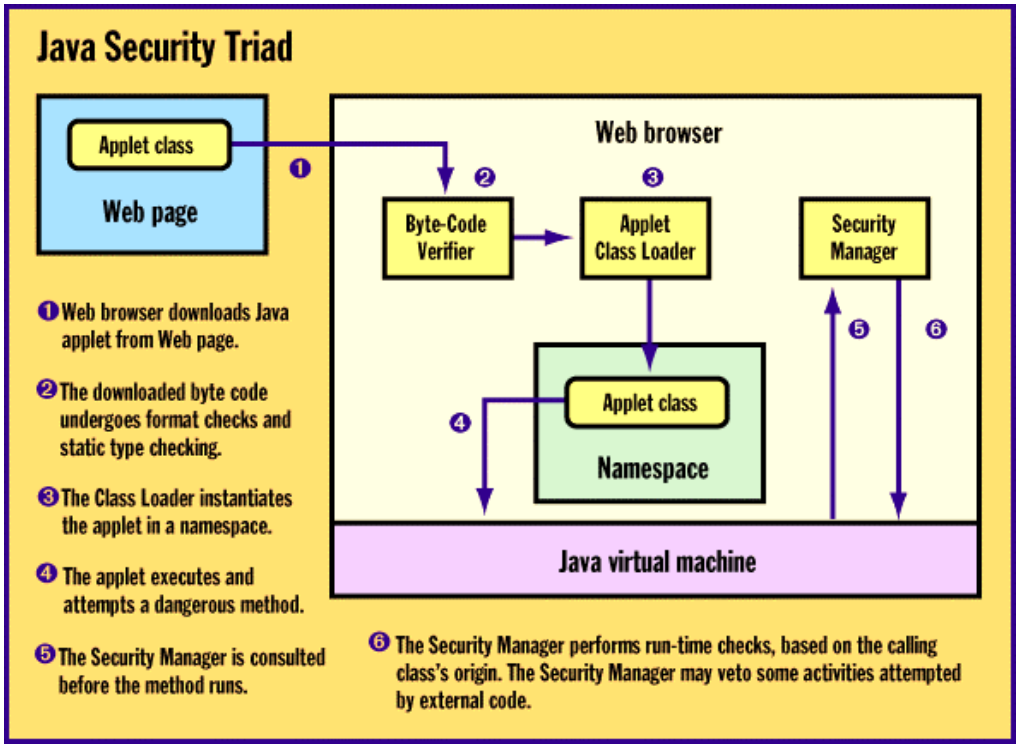
Η γλώσσα Java και ο μεταγλωττιστής της είναι η πρώτη γραμμή άμυνας**.** Η Java σχεδιάστηκε εξαρχής ώστε να είναι μια ασφαλής γλώσσα. Οι περισσότερες C-like γλώσσες, παρέχουν ευκολίες στον έλεγχο της πρόσβασης σε αντικείμενα, αλλά παρέχουν επίσης και δυνατότητες παραβίασης κανόνων πρόσβασης σε αντικείμενα, συνήθως με τη (κακόβουλη) χρήση των δεικτών (pointers). Έτσι έρχονται στο προσκήνιο δύο σημαντικές παραβιάσεις ασφαλείας. Η πρώτη συνίσταται στο ότι κανένα αντικείμενο δε μπορεί να προστατεύσει τον εαυτό του από έξωθεν τροποποίηση. Η δεύτερη είναι το γεγονός ότι μια γλώσσα με "ισχυρούς" δείκτες είναι πιο πιθανόν να έχει σοβαρά λάθη (bugs) που παραβιάζουν την ασφάλεια. Αυτά τα pointer bugs, όπου ένας "παραστρατημένος" δείκτης αρχίζει να τροποποιεί τη μνήμη που δεσμεύεται για άλλο αντικείμενο, αποτέλεσαν τις σοβαρότερες παραβιάσεις ασφαλείας στο Internet την περασμένη δεκαετία.

Η Java εξοστρακίζει αυτές τις απειλές, εξαλείφοντας εντελώς τους δείκτες από την αρχιτεκτονική της. Βέβαια, υπάρχουν δείκτες υπό την μορφή αναφορών σε αντικείμενα, αλλά ελέγχονται προσεκτικά προκειμένου να είναι ασφαλείς: οποιαδήποτε αναφορά στη μνήμη ελέγχεται εξονυχιστικά προτού επιτραπεί.

Η Τριάδα Ασφαλείας

Η ικανότητα της Java να "κατεβάσει" (download), να παράγει και να εκτελέσει κώδικα από έναν απομακρυσμένο υπολογιστή, είναι δίκοπο μαχαίρι . Οι σχεδιαστές της εισήγαγαν ένα μοντέλο ασφαλείας, το οποίο βασίζεται σε τρείς "αμυντικούς" μηχανισμούς: Ο **Byte-Code Verifier** (Πιστοποιητής Bytecode), ο **Applet Class Loader** (Φορτωτής Τάξης στο Applet), και ο **Security Manager** (Υπεύθυνος Ασφαλείας). Όλοι μαζί, οι τρεις αυτοί μηχανισμοί ασφαλείας επιτελούν ελέγχους πριν και κατά την εκτέλεση του προγράμματος, περιορίζοντας την πρόσβαση στο σύστημα αρχείων ή την πρόσβαση στο δίκτυο, όπως επίσης περιορίζουν την πρόσβαση και στα "ενδότερα" του browser. Κάθε ένας από τους μηχανισμούς αυτούς, εξαρτάται σε μεγάλο βαθμό από τους υπολοίπους, και πρέπει να επιτελεί το έργο του αποτελεσματικά, ώστε το μοντέλο

ασφαλείας να είναι σωστό.



Σχήμα 1 Η Τριάδα Ασφαλείας της Java

Στο σχήμα 1 φαίνεται πώς οι μηχανισμοί αυτοί ασφαλείας ενσωματώνονται στο περιβάλλον εργασίας της Java.

- Ο **Byte code Verifier** είναι ο πρώτος μηχανισμός που επικαλείται το μοντέλο ασφαλείας. Όταν ένα Java source πρόγραμμα μεταγλωττίζεται, μετατρέπεται σε bytecode για την JVM μηχανή, όπως έχουμε ήδη αναφέρει. Ο Verifier ελέγχει το μη έμπιστο αυτόν κώδικα, προκειμένου να διαπιστώσει αν "παίζει σύμφωνα με τους κανόνες". Πιο συγκεκριμένα, ο Verifier ελέγχει το byte code σε διαφορετικά επίπεδα. Στη συνέχεια, ελέγχει κάθε μέθοδο, εξασφαλίζοντας ότι το applet δεν επιχειρεί να εισάγει "ψεύτικους" δείκτες (pointers), να παραβιάσει δικαιώματα πρόσβασης σε αρχεία, να προκαλέσει υπερχείληση ή υποχείληση (overflow, underflow) σωρού (stack), να αποκτήσει τέλος πρόσβαση σε αντικείμενα χρησιμοποιώντας λανθασμένες πληροφορίες. Οι αναφορές σε αντικείμενα, κατόπιν του ελέγχου, μπορούν να μεταχειριστούν πλέον ως δυνατότητες (capabilities), εφόσον είναι αυθεντικές.

- Ο δεύτερος μηχανισμός ασφαλείας, είναι ο **Applet Class Loader**. Όταν μια καινούρια Τάξη "φορτώνεται" στο σύστημα, αναγκαστικά θα προέρχεται από μια εκ των τριών περιοχών δραστηριοτήτων: ο τοπικός υπολογιστής, το τοπικό δίκτυο (στο οποίο βρίσκεται ο υπολογιστής) που ενδεχομένως να βρίσκεται πίσω από firewall, το Internet. Κάθε μια από τις περιοχές αυτές τυγχάνει διαφορετικής μεταχείρισης από τον Class Loader. Συγκεκριμένα, ο Loader δεν επιτρέπει ποτέ μια Τάξη από μια "λιγότερο προστατευμένη" περιοχή να αντικαταστήσει μια τάξη από μια "περισσότερο προστατευμένη" περιοχή. Τα αρχεία συστήματος I/O για παράδειγμα, ορίζονται σε μια τοπική Java τάξη, δηλαδή ανήκουν στο realm "τοπικός υπολογιστής". Έτσι, καμιά Τάξη έξω από τον υπολογιστή (είτε από το τοπικό δίκτυο, είτε από το Internet) δεν πρέπει να πάρει τη θέση κάποιας από αυτές τις Τάξεις.

- Ο τρίτος μηχανισμός ασφαλείας είναι ο **Security Manager**. *SecurityManager* είναι μια abstract (αφηρημένη) Τάξη η οποία έχει προστεθεί στο Java σύστημα. Μια πραγματοποίηση (instance) κάποιας υποΤάξης της *SecurityManager* είναι ο τρέχων Security Manager. Έχει πλήρη έλεγχο σχετικά με το ποιές μέθοδοι, από ένα σύνολο ιδιαίτερα "επικίνδυνων" μεθόδων, επιτρέπεται να "καλούνται" από οποιαδήποτε δεδομένη Τάξη. Λαμβάνει υπ'όψην τα realms, την καταγωγή (προέλευση) της Τάξης και τον τύπο της Τάξης.

Για πρόσβαση σε αρχεία ή στο δίκτυο, ο χρήστης ενός Java-enabled browser μπορεί να επιλέξει μεταξύ τεσσάρων περιοχών ελέγχου:

απεριόριστη (unrestricted): επιτρέπει στα applets μα κάνουν ο,τιδήποτε.
firewall: επιτρέπει στα applets μέσα στο firewall να κάνουν ο,τιδήποτε.
πηγή (source): επιτρέπει στα applets να κάνουν ο,τιδήποτε, στον host προορισμού τους, η με άλλο applet από εκεί.
τ*οπική (local)*: Απαγορεύει εξολοκλήρου την πρόσβαση σε αρχεία και στο δίκτυο.

Πρέπει να τονιστεί, ότι ένας προγραμματιστής μπορεί να έχει πλήρη πρόσβαση στον Security Manager και θέτει τα δικά του κριτήρια παροχής προνομίων σε applets. Για πρόσβαση στο δίκτυο, είναι ευνόητο ότι περισσότερα κριτήρια είναι επιθυμητά. Για παράδειγμα, μπορούν να καθοριστούν διαφορετικές ομάδες έμπιστων domains, κάθε μια από τις οποίες θα έχει επιπρόσθετα προνόμια, όταν "φορτώνονται" applets από αυτήν την ομάδα. Επιπλέον, ορισμένες ομάδες μπορεί να είναι περισσότερο έμπιστες από κάποιες άλλες, ή ακόμα μπορεί να επιτρέπεται σε μια ομάδα να δεχθεί ένα καινούριο μέλος - παρέχοντάς του έτσι ίδια προνόμια. Σε κάθε περίπτωση, οι δυνατότητες είναι πολλές, αρκεί να υπάρχει ένας ασφαλής τρόπος αναγνώρισης του πραγματικού δημιουργού του applet.

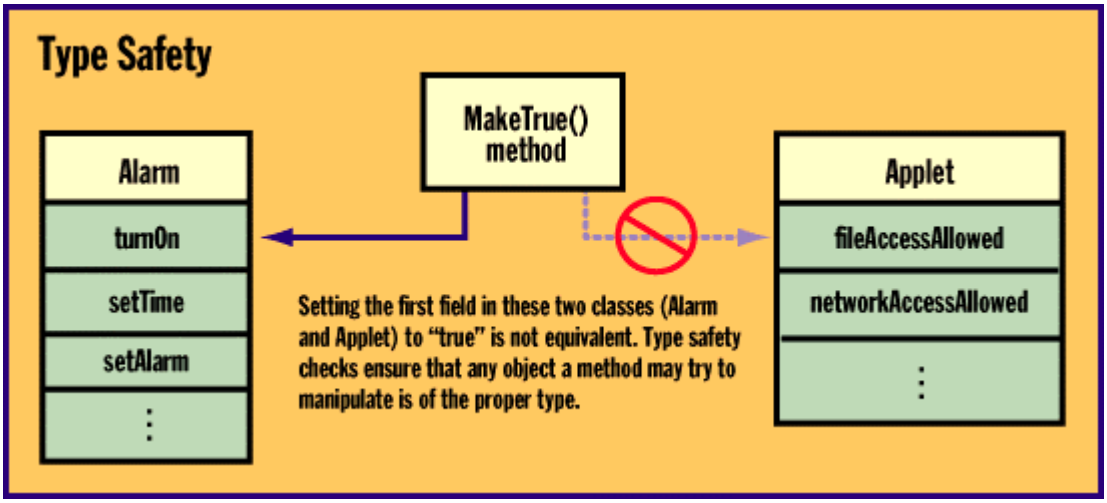
Ασφάλεια Τύπου

Οι τρεις μηχανισμοί του μοντέλου ασφαλείας της Java, στους οποίους αναφερθήκαμε, έχουν δημιουργηθεί ώστε να εξασφαλίζουν την **Ασφάλεια Τύπου** (type safety), η οποία σημαίνει ότι ένα πρόγραμμα μπορεί να εκτελεί συγκεκριμένες λειτουργίες σε συγκεκριμένα είδη αντικειμένων . Έτσι, τα Java προγράμματα δεν αποκτούν μη εξουσιοδοτημένη πρόσβαση στη μνήμη.

Πιό συγκεκριμένα, κάθε κομμάτι μνήμης είναι τμήμα ενός java αντικειμένου, και κάθε αντικείμενο έχει μια Τάξη. Για παράδειγμα, έστω ότι ένα applet για τη διαχείριση ημερολογίου χρησιμοποιεί τις Τάξεις Date (ημερομηνία), Appointment (ραντεβού), Alarm (Προειδοποίηση) και GroupCalendar. Κάθε Τάξη καθορίζει ένα συγκεκριμένο σύνολο λειτουργιών που επιτρέπονται στα αντικείμενα της αυτής Τάξης. Στο παράδειγμα αυτό, έστω ότι η Τάξη Alarm ορίζει μια λειτουργία *turn on*, αλλά η Τάξη Date δεν επιτρέπει την εκτέλεση της *turn on*. Η Τάξη Alarm αναπαρίσταται στη μνήμη,σύμφωνα με το σχήμα 2. Η Alarm καθορίζει τη λειτουργία *turnon*, που καθιστά το πρώτο πεδίο αληθές (true). Η Java run-time βιβλιοθήκη καθορίζει μια άλλη Τάξη που λέγεται Applet, της οποίας η διάταξη στη μνήμη φαίνεται επίσης στο σχήμα. Ας σημειωθεί ότι το πρώτο πεδίο της Applet είναι το *fileAccessAllowed*, που καθορίζει εαν το applet επιτρέπεται να έχει πρόσβαση σε αρχεία του σκληρού δίσκου ή όχι.

Ας υποθέσουμε τώρα ότι το πρόγραμμα επιχειρεί να εφαρμόσει τη *turnon* λειτουργία σε ένα Applet αντικείμενο. Εαν η *turnon* λειτουργία είναι επιτρεπτή, το πρόγραμμα καθιστά το πρώτο πεδίο του αντικειμένου αληθές (true). Δυστυχώς, εφόσον το αντικείμενο-στόχος είναι στην πραγματικότητα τύπου Applet, καθιστώντας το πρώτο

πεδίο αληθές επιτρέπει την πρόσβαση του applet στο σύστημα αρχείων. Το applet έτσι λανθασμένα—επιτρέπεται να τροποποιήσει ή ακόμα και να σβήσει αρχεία.



Σχήμα 2 Type Safety

Πώς η Java ενισχύει την Ασφάλεια τύπου

Η Java "στιγματίζει " κάθε αντικείμενο, συνδέοντάς το με ένα class tag. Ένας απλός τρόπος επιβολής Ασφάλειας Τύπου θα ήταν ο έλεγχος του tag για κάθε αντικείμενο, προτού εκτελεστεί μια λειτουργία σε αυτό, ώστε να εξασφαλιστεί ότι η Τάξη (class) του αντικειμένου επιτρέπει αυτήν τη λειτουργία. Αυτή η προσέγγιση λέγεται *δυναμικός έλεγχος τύπου* (dynamic type checking).

Παρότι αυτό το σχήμα δουλεύει, δεν είναι αποδοτικό. Τα προγράμματα κατ'αυτόν τον τρόπο αναλώνονται στον έλεγχο των class tags. Προκειμένου να βελτιωθεί η απόδοση, η Java χρησιμοποιεί *στατικό έλεγχο τύπου* (static type checking). Στατικός έλεγχος τύπου σημαίνει ότι το σύστημα Java ελέγχει ένα πρόγραμμα πριν το εκτελέσει και εξάγει προσεκτικά τα αποτελέσματα των tag-checking λειτουργιών. Εαν η Java μπορεί να συμπεράνει ότι μια συγκεκριμένη tag-checking λειτουργία θα πετυχαίνει πάντοτε, δεν υπάρχει λόγος να συνεχίσει να την εκτελεί. Έτσι, ο έλεγχος εξαλείφεται και η ταχύτητα του προγράμματος αυξάνεται. Ο Byte-Code Verifier είναι ένας αποτελεσματικός στατικός ελεγκτής τύπου.

Υπάρχει εντούτοις ένα πρόβλημα με την στατική type-checking στρατηγική της Java: είναι περίπλοκη. Παρότι οι σχεδιαστές της Java συνέλλαβαν ορθώς την στρατηγική αυτή, υπάρχουν πολλές λεπτομέρειες που πρέπει να είναι σωστές προκειμένου η Ασφάλεια Τύπου να είναι επιτυχής. Οποιοδήποτε λάθος σε κάποια από τις λεπτομέρειες, αφήνει μια μικρή αλλά ενδεχομένως σημαντική "τρύπα" στο σύστημα ασφαλείας. Ένας έξυπνος cracker που γίνεται γνώστης αυτής της "τρύπας" μπορεί να αρχίσει μια επίθεση *Σύγχισης Τύπου* (type-confusion attack). Ο cracker μπορεί να προκαλέσει μια κατάσταση παρόμοια με το Alarm/Applet παράδειγμα, όπου το πρόγραμμα έχει έναν τύπο αντικειμένου αλλά το σύστημα Java νομίζει ότι το αντικείμενο είναι άλλου τύπου.

4.3 Applets: Δικαιώματα και Υποχρεώσεις.

Ένα ιδιαίτερα "κομψό" αποτέλεσμα της ενσωματωμένης μεταφερσιμότητας της Java είναι ότι ένα Java πρόγραμμα συγκεκριμένου είδους (γνωστό και ως applet) μπορεί να επισυναφθεί σε μια Web σελίδα . Τα applets ενσωματώνονται στον HTML κώδικα της Web σελίδας και "ερμηνεύονται" από Web browsers που έχουν αυτήν τη δυνατότητα. Σήμερα οι πιο δημοφιλείς browsers, ο Netscape Communicator και ο

Microsoft Explorer αλλά και ο Hotjava της Sun "κατεβάζουν" (download) και αρχίζουν να εκτελούν οποιοδήποτε Java applet ανακαλύψουν ενσωματωμένο στην web σελίδα. Η Java, ως υλοποίηση της ιδέας του *"εκτελέσιμου περιεχομένου",* παρέχει αυτήν τη δυνατότητα παράγοντας κώδικα ανεξάρτητα με την πλατφόρμα στην οποία αυτός θα εκτελεστεί.

Υπάρχουν και άλλες ανταγωνιστικές υλοποιήσεις *"εκτελέσιμου περιεχομένου"*, όπως ActiveX, JavaScript, Safe-TCL, Telescript, Microsoft Word και Excel macros, και PostScript. Η Java όμως συνένωσε πολλούς κατασκευαστές λογισμικού "υπό την αιγίδα της" και αποτελεί την επικρατούσα τεχνολογία, τουλάχιστον προς το παρόν. Ανεξάρτητα με την υλοποίηση πάντως, η εκτέλεση κώδικα άγνωστης -συνήθως- προέλευσης εγγυμονεί κινδύνους και προκαλεί ανασφάλεια στην κοινότητα των χρηστών του Web. Τα applets μπορεί να γίνουν αρκετά εχθρικά προς τον χρήστη, ανάλογα με τα δικαιώματα που τους παραχωρούνται, και τους περιορισμούς οι οποίοι τους επιβάλλονται.

Τα εχθρικά Applets διακρίνονται σε δύο κατηγορίες: Τα *"επιθετικά"* applets, τα οποία μπορούν να προκαλέσουν σοβαρές παραβιάσεις στον τομέα της ασφάλειας, και τα *"πονηρά"* applets, τα οποία είναι περισσότερο ενοχλητικά παρά καταστροφικά . Παρότι λιγότερο επώδυνα, τα "πονηρά" applets είναι ύπουλα, αφού μπορούν να εκτελεστούν σε έναν υπολογιστή, με το που ο χρήστης του εισέλθει σε μια Web σελίδα.

Το Java run-time επιβάλλει περιορισμούς στο "τί μπορεί να κάνει ένα applet", ανάλογα και με τη version του JDK, όπως θα δούμε και στη συνέχεια.

Εντούτοις, ένα *"επιθετικό"* applet μπορεί να τροποποιήσει δεδομένα του σκληρού δίσκου, να φανερώσει "μυστικά" δεδομένα σε τρίτους, να "μολύνει" έναν υπολογιστή με ιό (virus), να εγκαταστήσει ένα trapdoor. Ένας cracker μπορεί να επιτύχει τον απόλυτο έλεγχο του υπολογιστή του χρήστη-θύματος. Εως σήμερα, γνωρίζουμε οκτώ (8) σοβαρά προβλήματα ασφαλείας σε Java εφαρμογές, τα οποία ποικίλλουν από προβλήματα στο DNS (Domain Naming System), εως type-confusion προβλήματα. Αυτές οι επιθέσεις δεν είναι υποθετικές. Κάθε επίθεση έχει υλοποιηθεί από την ομάδα Safe Internet Programming (SIP), γνωστή στην κοινότητα του Internet. Οι επιθέσεις αυτές παρουσιάζονται αναλυτικά στη συνέχεια του κεφαλαίου.

Το σίγουρο είναι πως η κακόβουλη χρήση των applets προϋποθέτει βαθειά γνώση των περίπλοκων δομών της γλώσσας Java και του Internet. Εντούτοις, ένα άτομο είναι αρκετό για να κατασκευάσει ένα εχθρικό applet. Εφόσον αυτό συμβεί, η πληροφορία θα διαδοθεί μέσω της κοινότητας των crackers, και τα αποτελέσματα θα είναι καταστροφικά.

Ακόμα και το λιγότερο *"πονηρό"* applet μπορεί να "λεηλατήσει" τον ιδιωτικό βίο ενός χρήστη του Web. *"Πονηρά"* applets μπορούν να στέλνουν mails εκ μέρους του χρήστη-θύματος σε οποιονδήποτε λέγοντας ο,τιδήποτε, μπορούν να χρησιμοποιούν την ΚΜΕ (CPU) του υπολογιστή του θύματος για δικό τους λογαριασμό, "ρίχνοντας" έτσι το σύστημα του θύματος και απορροφώντας όλους τους υπολογιστικούς πόρους. Επίσης, *"πονηρά"* applets μπορεί να είναι ιδιαίτερα ενοχλητικά: εκτελούν αρχεία ήχου για πάντα, καταγράφουν και παρακολουθούν (monitor) τις κινήσεις του χρήστη στο Web, εμφανίζουν στην οθόνη του ανεπιθύμητα γραφικά. Στο Web σήμερα είναι διαθέσιμες ολόκληρες συλλογές από *"πονηρά"* applets, για οποιονδήποτε ενδιαφερόμενο επιθυμεί να διαπιστώσει ιδίοις όμασι ποιά και πόσα applets αυτού του είδους υπάρχουν **.**

Προκειμένου να αντιμετωπίσει τα εχθρικά applets, η εταιρία JavaSoft αναζητεί λύσεις που θα βελτιώσουν την εικόνα του συστήματος ασφαλείας στο Java Development Kit (JDK) με το οποίο εφοδιάζει τους χρήστες του Internet. Αξίζει να αναφέρουμε πως στην πρώτη έκδοση του JDK τα applets δεν είχαν δικαίωμα ανάγνωσης, εγγραφής ή τροποποίησης δεδομένων σε τοπικά αποθηκευτικά μέσα του υπολογιστή που τα

εκτελούσε. Έτσι, υπήρχε το λεγόμενο **"**κουτί προστασίας**"** (sandbox) – το ασφαλές browser partition όπου τα applets εκτελούνταν κανονικά. Στις 19 Φεβρουαρίου του 1997, η JavaSoft ανακοίνωσε την έκδοση 1.1 του JDK , στην οποία έκδοση υπάρχουν αρκετές καινοτομίες. Συγκεκριμένα, τα applets συνοδεύονται πλέον από την ψηφιακή υπογραφή του δημιουργού τους, η ταυτότητα του οποίου εμφανίζεται στον χρήστη που μετέρχεται στην Web σελίδα η οποία περιέχει το applet. Ο χρήστης καλείται να αποφασίσει εαν επιθυμεί την εκτέλεση του applet πέρα από τα όρια του sandbox, οπότε το applet πλέον έχει δυνατότητες ανάγνωσης ή/και εγγραφής στον σκληρό δίσκο του υπολογιστή του, ή μπορεί (το applet) να αποκτήσει πρόσβαση σε URL διαφορετικό από το δικό του. Το applet, στο JDK 1.1 θα τρέξει στα πλαίσια ασφαλείας του sanbox, εαν ο χρήστης δεν εμπιστεύεται τον υπογράφοντα. Η διαδικασία της υπογραφής, δεν είναι πανάκεια. Δεν εξαλείφει τα καταστροφικά αποτελέσματα στα οποία μπορέι να οδηγήσει η εκτέλεση ενός applet, απλά λέει στο χρήστη-θύμα ποιός είναι υπεύθυνος για την καταστροφή αυτή.

Σε μελλοντικές υλοποιήσεις του JDK, αναμένεται η υιοθέτηση περισσότερο εκλεπτυσμένου ελέγχου επάνω σε ένα πρόγραμμα. Αναμένεται η υλοποίηση εκείνη του JDK, στην οποία ο χρήστης θα μπορεί να δίνει συγκεκριμένα δικαιώματα σε Java προγράμματα, να υϊοθετεί διαφορετικές πολιτικές ασφαλείας για κάθε πρόγραμμα και να τις μεταβάλλει όταν και όποτε αυτός θέλει. Για παράδειγμα, ο χρήστης θα μπορεί να "κρατάει" τα applets στα πλαίσια του sandbox εκτός και αν προέρχονται από ένα συγκεκριμένο "έμπιστο" site, ή να επιτρέπει σε κάποιο applet να διαβάζει (αλλά όχι να γράφει) στο σκληρό δίσκο.

4.4 Java: ασφαλής, ή μήπως επικίνδυνη;

Στη συνέχεια, περιγράφουμε αναλυτικά τις κατηγορίες στις οποίες μπορούν να ταξινομηθούν οι επιθέσεις με κακόβουλη χρήση της Java και των προγραμμάτων της, σε συνάρτηση πάντα με την υλοποίηση του Java runtime περιβάλλοντος αλλά και την ανθεκτικότητα των browsers που την υποστηρίζουν .

4.4.1 Επιθέσεις Άρνησης Υπηρεσίας (denial of service attacks)

Η επιθέσεις αυτές συνιστούν την "εξάντληση" της ΚΜΕ και την δέσμευση μνήμης του υπολογιστή-θύματος, μέχρι την τελική κατάρρευσή του. Επιπλέον, ένα applet μπορεί να μπλοκάρει κρίσιμα "κομμάτια" του browser που το εκτελεί, καθιστώντας τον ανενεργό.

Υπάρχουν δύο λόγοι που καθιστούν τις denial of service επιθέσεις δύσκολο να αντιμετωπιστούν. Πρώτον, μία επίθεση μπορεί να προγραμματιστεί να συμβεί μετά από κάποιο χρονικό διάστημα, ούτως ώστε να εκδηλωθεί όταν ο χρήστης βρίσκεται σε διαφορετική σελίδα από αυτή στην οποία είχε εκτελεστεί το applet. Δεύτερον, η επίθεση αυτού του είδους μπορεί να προκαλέσει *"υποβάθμιση της υπηρεσίας"* παρά άρνηση υπηρεσίας. Υποβάθμιση υπηρεσίας σημαίνει ότι η ο browser υπολειτουργεί, χωρίς να αναστέλλεται η λειτουργία του. Για παράδειγμα, η επίθεση "μπλοκαρίσματος" στην οποία αναφερθήκαμε, θα μπορούσε να χρησιμοποιηθεί στο να μπλοκάρει ένα κρίσιμο κομμάτι στου συστήματος για κάμποση ώρα, στη συνέχεια να το αποδεσμεύσει, να το ξαναμπλοκάρει, και ούτω καθ' εξής. Το αποτέλεσμα θα ήταν ένας browser που λειτουργεί πάρα πολύ αργά.

4.4.2 Πληροφορίες διαθέσιμες στα applets

Σε παλαιότερες εκδόσεις των browser HotJava (1.0) και Netscape Navigator (2.0), η κλήση συστήματος *accept ( )*, η οποία χρησιμοποιείται προκειμένου να δέχεται μία αίτηση για σύνδεση με κάποιον host, ύστερα από αίτηση του τελευταίου, δεν

προστατεύονταν σωστα, με αποτέλεσμα κάποιο "κακόβουλο" applet να ήταν ικανό να συνδεθεί με οποιονδήποτε browser, αρκεί να ήξερε τη διεύθυνσή του στις τελευταίες εκδόσεις των δύο browser η *accept ( )* προστατεύεται καταλλήλως.

Στον browser HotJava, για παράδειγμα (έκδοση 1.0) οι περισσότερες απόπειρες ενός applet να αναγνώσει ή να τροποποιήσει δεδομένα στο τοπικό σύστημα αρχείων, οδηγούν σε ένα dialog box το οποίο καλεί τον χρήστη να δώσει ή όχι τη συγκατάθεσή του. Ορισμένες Λίστες Ελέγχου Πρόσβασης (Access Control Lists) καθορίζουν πού μπορούν να πραγματοποιηθούν αναγνώσεις (read) ή/και εγγραφές (write) αρχείων ή καταλόγων χωρίς την συγκατάθεση του χρήση. Εξ' ορισμού, η write ACL είναι άδεια και η read ACL περιέχει τον κατάλογο (directory) στον οποίο βρίσκεται η βιβλιοθήκη του HotJava και συγκεκριμένα MIME mailcap αρχεία. Η read ACL επίσης περιέχει τον public_html κατάλογο του χρήστη, ο οποίος μπορεί να περιέχει κρίσιμες εμπιστευτικές πληροφορίες. Αυτό επιτρέπει σε ένα applet να καταστρέψει αρχεία τα οποία χρησιμοποιούνται από άλλες Windows εφαρμογές, εαν φυσικά το applet μπορεί να "μαντέψει" τα ονόματα των αρχείων αυτών. Το λιγότερο που μπορεί να κάνει ένα τέτοιο applet είναι να καταναλώσει όλον τον ελεύθερο χώρο στο σκληρό δίσκο.

4.4.3 Λάθη Υλοποίησης (Implementation Errors)

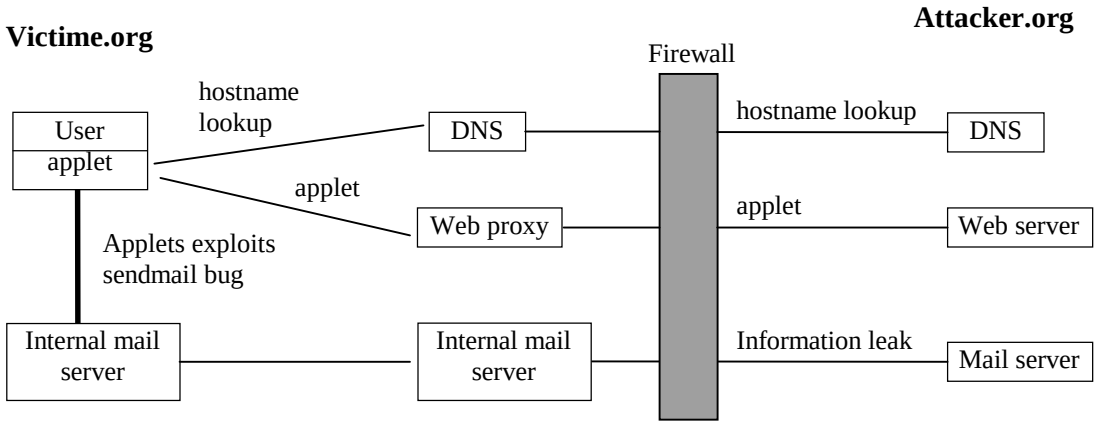
Ορισμένα λάθη προκύπτουν από την λανθασμένη υλοποίηση του browser ή του Java υποσυστήματος.

DNS αδυναμίες

Στις υλοποιήσεις των JDK (1.02) και Netscape (2.0) εμφανίζεται ένα σοβαρό πρόβλημα στην εφαρμογή της πολιτικής ασφαλείας σύμφωνα με την οποία "ένα applet μπορεί να εκκινήσει TCP/IP σύνδεση μονάχα με τον server από τον οποίο φορτώθηκε". Η πολιτική αυτή συνοψίζεται στα εξής βήματα:

1) Πάρε όλες τις IP διευθύνσεις του hostname από το οποίο προήλθε το applet.
2) Πάρε όλες τις IP διευθύνσεις του hostname με το οποίο προσπαθεί να συνδεθεί το applet.
3) Εάν οποιαδήποτε διεύθυνση του πρώτου συνόλου ταυτίζεται με οποιαδήποτε διέθυνση του δευτέρου συνόλου, επέτρεψε τη σύνδεση. Ειδάλλως, εμπόδισε τη σύνδεση

Το πρόβλημα προκύπτει στο δεύτερο βήμα: το applet μπορεί να ζητήσει να συνδεθεί με οποιοδήποτε hostname στο Internet, επομένως μπορεί να γνωρίζει ποιός DNS server παρέχει τη δεύτερη λίστα των IP διευθύνσεων. Οι πληροφορίες από τον αναξιόπιστο αυτόν DNS server χρησιμοποιούνται στην απόφαση του συστήματος ασφαλείας. Όμως, ένας "κακόβουλος" χρήστης ενδέχεται να κατασκευάσει έναν DNS server που ψεύδεται. Συγκεκριμένα, μπορεί να ισχυριστεί (ο server) ότι το τάδε όνομα host (hostname) έχει τη δείνα IP διεύθυνση. Χρησιμοποιώντας τα ψευδή αυτά ζευγάρια διευθύνσεων, ένα applet μπορεί να συνδεθεί με οποιονδήποτε υπολογιστή του Internet επιθυμεί. Αυτού του είδους οι επιθέσεις είναι πολύ επικίνδυνες, ιδιαίτερα όταν ο browser "τρέχει" πίσω από firewall, διότι το "κακόβουλο" applet μπορεί να προβεί σε επίθεση εναντίον οποιουδήποτε υπολογιστή βρίσκεται πίσω από το firewall. Μια τέτοια επίθεση φαίνεται στο σχήμα 5.



Σχήμα 5 DNS παράκαμψη της Java

Όπως φαίνεται και στο σχήμα, ένα applet ταξιδεύει από το attacker.com στο victim.org μέσω νομίμων καναλιών. Το applet στη συνέχεια ζητάει να συνδεθεί στο foo.attacker.com, ο οποίος σύμφωνα με τον ψευδή DNS server του attacker.com είναι ο εσωτερικός mail server του victim.org. Ο στόχος και τα αποτελέσματα της επίθεσης είναι προφανή.

4.5 ActiveX

Το ActiveX είναι ένα πρότυπο επικοινωνίας μεταξύ ολοκληρωμένων στοιχείων εκτελέσιμου κώδικα . Με άλλα λόγια είναι ένας τρόπος "συγκόλλησης" έτοιμων τμημάτων κώδικα για την πιο εύκολη και ταχεία ανάπτυξη πολύπλοκων εφαρμογών. Αυτό σημαίνει πως αν κάποιος έχει στα χέρια του μια σειρά από components, στοιχεία κώδικα δηλαδή, τα οποία διεκπεραιώνουν κάποιες απλές λειτουργίες (π.χ κάποιο component που αναλαμβάνει να εμφανίσει έναν απλό text editor στην οθόνη, ένα άλλο που στέλνει και διαβάζει e-mails από το Internet και άλλα που χειρίζονται στοιχεία του user interface του λειτουργικού: λίστες, buttons, checkboxes κ.λ.π), μπορεί να τα "δέσει" μεταξύ τους, χρησιμοποιώντας την τεχνολογία του ActiveX, και να κατασκευάσει μια ολοκληρωμένη εφαρμογή (στο παράδειγμά μας, έναν απλό Internet mailer).

Η βασική ιδέα πίσω από το ActiveX λοιπόν, είναι η δυνατότητα εκμετάλλευσης έτοιμου κώδικα από οποιοδήποτε πρόγραμμα, γραμμένου σε οποιαδήποτε γλώσσα, ώστε η ανάπτυξη software να διευκολύνεται όσο το δυνατό περισσότερο. Στο πνεύμα αυτό, η Microsoft δημιούργησε το ActiveX στις αρχές του 1996 και το ενσωμάτωσε βαθιά μέσα ~~στα 32-bit λειτουργικά της.~~ Το ActiveX, για να λειτουργήσει, βασίζεται σε ένα άλλο πρότυπο της Microsoft, το COM (Component Object Model), ένα πρότυπο κατασκευής software components τα οποία "εκθέτουν" ιδιότητες και μεθόδους μεταχείρισής τους με το πρότυπο του ActiveX. Το COM "χτίστηκε" επάνω στην τεχνολογία του OLE (Object Linking & Embedding), παίρνοντας από αυτό όλα τα "καλά του στοιχεία" και εξαλείφοντας τις αδυναμίες του. Το πρόβλημα με το OLE ήταν ότι δεν επέτρεπε την επικοινωνία από ένα αντικείμενο προς το αντικείμενο που το περιείχε, καθιστώντας το άχρηστο για τη δημιουργία controls, τα οποία έπρεπε να είναι σε θέση να στέλνουν κατά βούληση πληροφορίες προς τα αντικείμενα που τα περιείχαν.

Έχοντας ως βάση αυτές τις τεχνολογίες, η Microsoft προχώρησε στην ανακοίνωση της Active platform, μιας πλατφόρμας-φορέα Internet εφαρμογών, η οποία αποτελείται από τρία βασικά στοιχεία: Dynamic HTML, scripting και ActiveX

components. Η Active platform έχει server και client τμήματα. Στην πλευρά του server χρησιμοποιούνται scripting engines και ActiveX components για την παραγωγή HTML σελίδων, οι οποίες αποστέλλονται στον client και περιέχουν scripting κώδικα και αναφορές σε ActiveX controls. Ο client, κατόπιν, εμφανίζει τη σελίδα μαζί με όσα controls περιέχει και τα ελέγχει μέσα από τις scripting εντολές που συμπεριλαμβάνονται στη σελίδα. Η σελίδα έχει τη δυνατότητα να μεταβάλλει την όψη και το περιεχόμενό της, χωρίς την περαιτέρω σύνδεση ανάμεσα στον client και τον server.

Το πιο σημαντικό στοιχείο-κλειδί για την Active platform είναι τα ActiveX controls. Είναι αυτά που εγγυώνται την επεκτασιμότητα και προσαρμογή του client τμήματος στις περιστάσεις και χωρίς αυτά η Active platform χάνει ένα μεγάλο μέρος από τα πλεονεκτήματά της έναντι ενός τυπικού Web browser. Το κυριότερο πρόβλημα με τα ActiveX controls είναι πως δεν είναι ανεξάρτητα από την πλατφόρμα στην οποία τρέχουν. Σε αυτό το σημείο μπορεί να υπάρξει μια παρανόηση: Το ActiveX είναι μια τεχνολογία, η οποία δε βασίζεται σε κάποια συγκεκριμένη αρχιτεκτονική, και μπορεί να υλοποιηθεί σε οποιοδήποτε λειτουργικό σύστημα. Τα ActiveX controls όμως, είναι κώδικας εκτελέσιμος, ο οποίος λειτουργεί μόνο στην πλατφόρμα στην οποία δημιουργήθηκε και με την υλοποίηση του ActiveX ή οποία χρησιμοποιήθηκε. Ως εκ τούτου, τα ActiveX controls εξαρτώνται από τον υπολογιστή που φιλοξενεί τον Active platform client κι έτσι δεν μπορούν να ανταγωνιστούν σε αυτόν τον τομέα τεχνολογίες όπως η Java.

4.5.1 ActiveX: Μήπως ακόμα μια απειλή;

Η ασφάλεια στο ActiveX βασίζεται στην ανθρώπινη κρίση. Τα προγράμματα ActiveX (ή ActiveX controls) συνοδεύονται από μια ψηφιακή υπογραφή από το συγγραφέα του προγράμματος, και οποιουδήποτε άλλου αποφασίζει να υποστηρίξει ή επιδοκιμάσει το πρόγραμμα. Η ψηφιακή υπογραφή αποτελεί το ψηφιακό ισοδύναμο της ανθρώπινης υπογραφής. Ο browser αποφασίζει για το εαν η υπογραφή που συνοδεύει το control είναι αυθεντική και πληροφορεί τον χρήστη για την πραγματική ή όχι ταυτότητα του προσώπου (ή φορέα) που υπέγραψε το πρόγραμμα. Στη συνέχεια ο χρήστης καλείται να αποφασίσει εαν θα δεχθεί ή όχι την εκτέλεση του ActiveX στον υπολογιστή του.

Το φλέγων σημείο στην ασφάλεια του ActiveX, είναι ότι εαν ο χρήστης δεχθεί την εκτέλεση του ActiveX προγράμματος στον υπολογιστή του, το πρόγραμμα δεν έχει κανέναν απολύτως περιορισμό.

Στις 7 Φεβρουαρίου 1997, το Chaos Computer Club, μια ομάδα hackers από το Αμβούργο της Γερμανίας, έκαναν επίδειξη των καταστροφικών αποτέλεσμάτων που μπορεί να έχει η "κακόβουλη" χρήση ενός ActiveX προγράμματος (control) . Παρουσίασαν στην γερμανική τηλεόραση ένα ActiveX control το οποίο είναι ικανό να μεταφέρει χρήματα από έναν τραπεζικό λογαριασμό σε έναν άλλον, και αυτό χωρίς τη χρήση πρωσοπικού αριθμού ταυτότητας (PIN). Μόλις γίνει downloaded από ένα Web site, το πρόγραμμα "ψάχνει" στον υπολογιστή του θύματος για το δημοφιλές λογισμικό συναλλαγών "Quicken" της εταιρίας Intuit . Το ActiveX control, στη συνέχεια "ξεγελά" το Quicken αναγκάζοντάς τον να μεταφέρει χρήματα από τον ένα λογαριασμό στον άλλον, την επόμενη φορά που συνδέεται με μια τραπεζιτική υπηρεσία.

Το προηγούμενο πρόβλημα καταδεικνύει ότι, σε αντίθεση με την Java, τα ActiveX controls, τα οποία εκτελούνται κυρίως μέσα από τον Internet Explorer browser της Microsoft, μπορούν να κάνουν ο,τιδήποτε στον υπολογιστή του θύματος που δέχεται την εκτέλεσή τους ακόμα και να εγκαταστήσουν έναν ιό. Βέβαια, η Microsoft έχει ήδη ανακοινώσει προ πολλού ένα σύστημα "λογοδότησης" (accountability system) το οποίο καλείται **Authenticode** και είναι ενσωματωμένο στον Internet Explorer. Σύμφωνα με το σύστημα αυτό, οι εκδότες λογισμικού (software publishers)

υπογράφουν ψηφιακά τα controls τους. Εαν ένα control διαπράξει κάτι "κακό" στον υπολογιστή ενός χρήστη, ο εκδότης μπορεί να εντοπιστεί και να διωχθεί ποινικά. Με άλλα λόγια, το σύστημα Authenticode δεν προστατεύει από "πονηρό" κώδικα, απλά καθιστά εύκολη την ανεύρεση του δημιουργού του.

Ο κύριος κίνδυνος στο ActiveX είναι όταν ο χρήστης πάρει μια λάθος απόφαση και αποφασίσει να δεχθεί την εκτέλεση του προγράμματος. Μπορεί για παράδειγμα, κάποιος που ο χρήστης εμπιστεύεται, να αποδειχθεί ότι δεν άξιζε της εμπιστοσύνης του. Ο μεγαλύτερος όμως κίνδυνος είναι όταν το πρόγραμμα υπογράφεται από κάποιον για τον οποίο ο χρήστης δεν γνωρίζει τίποτα. Το δέλεαρ είναι μεγάλο, ιδιαίτερα εαν το πρόγραμμα "υπόσχεται" όμορφα animations, καλή μουσική ή άλλα happenings. Έτσι, υπάρχουν περιπτώσεις που ο χρήστης σκεφτεται: "*Οι πιθανότητες το συγκεκριμένο πρόγραμα να είναι "κακό", είναι πολύ λίγες, οπότε γιατί να μην το δεχθώ; Ούτως ή άλλως χθες εκτέλεσα τρία προγράμματα και τίποτα δεν πήγε στραβά*". Ακόμα και αν ο κίνδυνος δεν είναι πιθανός, γίνεται περισσότερο ορατός όταν επαναλαμβάνονται αλόγιστα αποδοχές ActiveX προγραμμάτων αμφιβόλου προέλευσης από το χρήστη. Η μοναδική λύση να αποφευχθεί αυτό το σενάριο είναι κάποιος να απορρίπτει όλα τα ActiveX controls που συναντάει στο Web. Ποιός όμως έχει την αυτοπειθαρχία να υιοθετήσει μια τέτοια πολιτική;

4.5.2 Java εναντίον ActiveX

Η Java και το ActiveX είναι δύο συστήματα που επιτρέπουν στους χρήστες του Web να επισυνάπτουν προγράμματα στην σελίδα τους. Τα συστήματα αυτά αρέσουν στους χρήστες γιατί τους επιτρέπουν να δημιουργούν περισσότερο "δυναμικές" και αλληλεπιδραστικές σελίδες. Εντούτοις, τόσο η Java όσο και το ActiveX εισάγουν κάποια προβλήματα σε θέματα ασφαλείας, καθώς επιτρέπουν εκτός των άλλων σε εχθρικά προγράμματα να εκτελούνται στον υπολογιστή οποιουδήποτε επισκέφτεται μια σελίδα. Το downloaded πρόγραμμα μπορεί να προσπαθήσει να καταστρέψει δεδομένα στον υπολογιστή, ή ενδεχομένως να εγκαταστήει έναν ιό. Τόσο η Java, όσο και το ActiveX υϊοθετούν μέτρα ασφαλείας εναντίον τέτοιων ανεπιθύμητων καταστάσεων. Τελευταία υπάρχει μια "κόντρα" μεταξύ ειδημόνων στην κοινότητα των χρηστών του Web σχετικά με το ποιά τεχνολογία είναι περισσότερο ασφαλής.

Όπως είναι γνωστό, τόσο τα Java applets όσο και τα ActiveX controls συνοδεύονται απο ψηφιακές υπογραφές, που αυθεντικοποιούν τους δημιουργούς τους στον χρήστη που τα συναντάει σε Web σελίδες. Η διαφορά μεταξύ τους είναι ότι τα Java applets μπορούν να κρατηθούν μέσα στο sandbox χωρίς να αποκτούν δικαιώματα εγγραφής ή ανάγνωσης, αρκεί βέβαια το software του sandbox να έχει υλοποιηθεί σωστά. Αντίθετα, το ActiveX πρόγραμμα με το που γίνει αποδεκτό, μπορεί να δράσει χωρίς περιορισμούς. Σε αυτό το σημείο λοιπόν, διαφαίνεται η υπεροχή της Java στα θέματα ασφαλείας.

Επίσης, ένας Java-enabled browser, θα μπορούσε να κρατήσει records με όλες τις επικίνδυνες λειτουργίες τις οποίες πραγματοποιεί ένα πρόγραμμα, καθιστώντας πιο εύκολη την απεμπλοκή από μια δυσάρεστη κατάσταση, ή τη διόρθωση των αποτελεσμάτων που επέφερε (Οι browsers που κυκλοφορούν αυτήν τη στιγμή δεν έχουν τέτοια δυνατότητα, αλλά θα μπορούσαν να την αποκτήσουν, λόγω της φύσης της Java).

4.6 Ελαττώνοντας τα ρίσκα

Κάποιοι ειδικοί τονίζουν, ίσως ειρωνικά, ότι η Java είναι η γλώσσα η οποία θα επιλεγεί ώστε να δημιουργηθεί ο πρώτος machine-independed ιός . Από την άλλη, πολλοί υπεύθυνοι δικτύων αισθάνονται ότι η Java είναι η λύση στα προβλήματά τους,

λόγω της ευκαμψίας που διαθέτει. Κάτι ανάλογο υποστηρίζεται και για το ActiveX.

Ακουγεται η άποψη ότι υπάρχουν προβλήματα ασφαλείας, περισσότερο σημαντικά από αυτά που σχετίζονται με τη Java. Ως παραδείγματα αναφέρονται οι Word επεξεργαστές, το Domain Name System, το MIME (Multipurpose Internet Mail Extension) και οι Web browsers. Οι DNS παραβιάσεις κάνουν δύσκολη την επιβεβαίωση της καταγωγής μιας σύνδεσης στο Internet. Το MIME επιτρέπει σε εκτελέσιμα δυαδικά δεδομένα να μετακινούνται όπως το κείμενο ή τα μηνύματα mail.

Φιλτράρισμα

Τόσο η Sun (Java), όσο και η Microsoft Corp. (ActiveX) υποστηρίζουν ότι οι applets τεχνολογίες τους είναι ασφαλείς, αλλά είναι δύσκολο να πείσουν αυτούς που εντρυφούν σε θέματα ασφαλείας . Οι περισσότεροι administrators, είναι σκεπτικοί απέναντι στην Java και καταδικαστικοί απέναντι στο ActiveX. Ένας λόγος που τα ActiveX προκαλούν περισσότερο φόβο, είναι ίσως το γεγονός ότι η τεχνολογία ActiveX είναι άρρηκτα συνδεδεμένη με την Windows οικογένεια λειτουργικών συστημάτων οπότε τα προγράμματα έχουν μεγαλύτερη πρόσβαση σε όποιο host έχει εγκατεστημένα Windows. Έτσι, ορισμένοι πήραν την απόφαση να "τραβήξουν το καλώδιο από την πρίζα", στερώντας από τους τοπικούς χρήστες του δικτύου καινούριες εφαρμογές και των δύο (Java και ActiveX) τεχνολογιών.

Πολλά firewalls προσφέρουν τη δυνατότητα "μπλοκαρίσματος" όλων των ActiveX και Java applets που επιχειρούν να μπουν στο δίκτυο. Αλλά, αυτή η λογική του "όλα-ή-τίποτα", δεν είναι η καλύτερη λύση που θα περίμενε κανείς, καθώς η τεχνολογία εξελίσσεται με τέτοιο ρυθμό, ώστε οι Web σελίδες να τείνουν να γίνουν ένα framework για suites εφαρμογών όπως το Microsoft Office. Με την ελπίδα, ότι θα παρασύρουν τους administrators μακριά από τη λογική του "όλα-ή-τίποτα", υπάρχουν αυτήν τη στιγμή ορισμένα screening προϊόντα, τόσο για τα Java applets όσο και για τα ActiveX controls. Η Εταιρία Finjan Software Inc . έχει από το 1996 και μετά προβεί σε μια σειρά ανακοινώσεων applet-analyzing και applet- screening προϊόντων τόσο για το desktop όσο και για το Internet Gateway, ενώ πολλοί κατασκευαστές firewalls έχουν συμβεβληθεί μαζί της και ενσωματώνουν την τεχνολογία της στα προϊόντα τους. Οι εφαρμογές αυτές, επειδή είναι όψιμες στον χώρο του Web όπως άλλωστε και η Java και το ActiveX, θα κριθούν με το πέρασμα του χρόνου. Οποιαδήποτε άλλη κρίση σχετικά με την αποτελεσματικότητά τους, θα ήταν βεβιασμένη.

Κατάλληλη διαμόρφωση των browsers

Ο Internet Explorer παρέχει στους χρήστες τη δυνατότητα να προειδοποιούνται πριν εκτελεστούν applets στον υπολογιστή τους, όπως και τη δυνατότητα να μην επιτρέπουν καθόλου την εκτέλεσή όλων των applets. Επίκειται στον χρήστη, λοιπόν, το αν θα επιλέξει τη μία ή την άλλη λύση. Στην γενικότερη περίπτωση προστασίας του δικτύου και των χρηστών του, υπάρχουν κάποια βήματα που πρέπει να ακολουθούνται:

- Όλοι οι χρήστες πρέπει να έχουν τον ίδιο browser εγκατεστημένο στον υπολογιστή τους, η έκδοση του οποίου θα πρέπει να είναι η πιο πρόσφατη. Τόσο η Netscape όσο και η Microsoft, αλλάζουν συχνά τις εκδόσεις των browser τους, γι'αυτό ο administrator του δικτύου θα πρέπει να φροντίζει ότι οι χρήστες έχουν την τελευταία έκδοση.

- Οι χρήστες του δικτύου πρέπει να είναι ενημερωμένοι για τα χαρακτηριστικά ασφαλείας που διαθέτει ο browser. Στον **Internet Explorer**, οι χρήστες επιλέγουν "Options" από το μενού "View" και στη συνέχεια επιλέγουν το "Security" tab.

Επιλέγοντας το κουμπί “Safety Level” και έπειτα την επιλογή “High”, εξασφαλίζεται ότι οι χρήστες θα προειδοποιούνται για την προέλευση των applets, πριν αυτά εκτελεστούν.

4.7 Σκέψεις για τη Java Λάθος προσανατολισμός

Παρά την έξαρση που επικρατεί αυτήν τη στιγμή στους επιστημονικούς κύκλους σχετικά με την ασφάλεια στο Internet, και τον μεγάλο αριθμό βιβλίων και συγγραμμάτων που βλέπουν καθημερινά το φως της δημοσιότητας, η ουσία παραμένει η ίδια: Οι περισσότερες συζητήσεις και απόψεις δίνουν έμφαση σε κινδύνους οι οποίοι δεν έχουν υλοποιηθεί στην πράξη.Για παράδειγμα, η Java λέγεται ότι είναι ασφαλής επειδή τα Java applets δεν μπορούν να διαβάσουν ή να εγγράψουν σε αρχεία, στην client μηχανή.

Σε ένα κατανεμημένο σύστημα, συνήθως δεν παίζει τόσο μεγάλο ρόλο αν είναι ασφαλής η πληροφορία, εκτός και αν δεν είναι δυνατή η παροχή της. Η επιθέσεις Άρνησης Υπηρεσίας (Denial of Service) είναι πολύ αποτελεσματικές. Έτσι, όταν ένας υπολογιστικός πόρος εκτίθεται στο Internet, με τις επιθέσεις αυτού του είδους είναι δυνατός ο κορεσμός του σε τέτοιο σημείο ώστε οι νόμιμοι χρήστες να παύουν να εξυπηρετούνται.

Ουσιαστικά, ο κορεσμός υπολογιστικών πόρων είναι ίσως η μεγαλύτερη απειλή στην εμπορική βιωσιμότητα στο Internet. Στο τεύχος Απριλίου 1996 του περιοδικού Wired υπάρχει ένα άρθρο στο οποίο περιγράφεται ένα “φανταστικό” άρθρο ενός άλλου περιοδικού, δέκα μήνες αργότερα, το οποίο θα αναφερόνταν στο θάνατο του Web. Σύμφωνα με αυτήν την αναφορά, μόνο ένα 10% των κλήσεων μιας Web σελίδας πραγματοποιείται από χρήστες που επιθυμούν να δουν τα περιεχόμενά της, ενώ το 90% των κλήσεων πραγματοποιείται από Web-Searching εργαλεία αναζήτησης. Αυτά τα indexing προγράμματα, σχεδιασμένα ώστε να ανιχνεύσουν το Web και να ταξινομήσουν τους πόρους του, μπορούν να επιδείξουν αναρίθμητους συνδυασμούς ταχύτητας και ηλιθιότητας. Μπορούν για παράδειγμα, να συναντήσουν ένα button που δημιουργεί μια πανομοιότυπη σελίδα, να πραγματοποιήσουν το ρομποτικό ισοδύναμο του να “πατήσουν” αυτό το button, και να επαναλαμβάνουν αυτήν τη συμπεριφορά αιωνίως, κάνοντας ένα ατέρμονο ταξίδι από μια Web σελίδα στο είδωλό της.

Προστίθοντας στο Web τη δύναμη μιας γλώσσας όπως η Java, δεν οδηγεί στην αποτροπή παρόμοιων δυνητικών απωλειών της “ικανότητας” του δικτύου. Τα abstractions της Java, παρότι ιδιαίτερα χρήσιμα σε πολλές εφαρμογές, δεν έχουν την εγγενή δύναμη να βοηθήσουν τους προγραμματιστές να δημιουργήσουν περισσότερο έξυπνους πράκτορες (intelligent agents).

Τα παιχνίδια που παίζουν οι άνθρωποι

Μία εφαρμογή Java μπορεί να χρησιμοποιήσει “ύπουλα” μέσα προκειμένου να αυξήσει το πλεονέκτημά της σε μια συναλλαγή, χωρίς να επιδίδεται σε πράξεις που είναι, ας πούμε, παράνομες. Οι άνθρωποι πραγματοποιούν συναλλαγές με αμοιβαία ανεξάρτητους στόχους, και εργαλεία όπως η Java δίνουν στους προγραμματιστές την ευκαιρία να είναι αρκετά διακριτικοί ώστε να πραγματοποιήσουν τους στόχους τους με μη διαφανείς τρόπους.

Οι ευθύνες

Ένα άλλο θέμα το οποίο συγκεντρώνει μεγάλη προσοχή στις μέρες μας είναι αυτό της ασφάλειας σημαντικών δεδομένων όπως αριθμοί πιστωτικών καρτών. Έχουν προταθεί πολλά σχήματα για παράδειγμα, η χρήση αλγορίθμων που αποδεικνύουν ότι το ένα απο τα συναλλασσόμενα μέρη κατέχει μια ποσότητα πληροφορίας χωρίς να την αποκαλύψει (αλγόριθμοι μηδενικής γνώσης). Αυτά τα σχήματα προφυλάσσουν τη

συναλλαγή από άτομα που δεν συμμετέχουν στη συναλλαγή. Οι Υπεύθυνοι ασφαλείας δικτύων, που θεωρούν αυτά τα σχήματα ως επαρκή, αγνοούν συστηματικά τις "απάτες με πιστωτικές κάρτες" που γίνονται από τον έμπορο που συμμετέχει στη συναλλαγή.

Η συμμετοχή ενός προσώπου σε μια συναλλαγή, δεν σημαίνει ότι το πρόσωπο αυτό είναι έμπιστο. Άλλα δυνητικά προβλήματα, που είναι εξωγενή ως προς την Java, οφείλονται στις αλληλεπιδράσεις της με εργαλεία που την υποστηρίζουν, όπως οι Web browsers –οι οποίοι μπορεί να κάνουν χρήση cashing μηχανισμών, για παράδειγμα, που κατακρατούν σε ένα σχήμα ανασφαλή πληροφορία που θα έπρεπε να είναι ασφαλής.

Όπως και σε κάθε άλλη τεχνολογία επεξεργασίας πληροφορίας, η γνώση της Java για το σύστημα γύρω από αυτήν είναι περιορισμένη. Οι Java εφαρμογές δεν έχουν την εγγενή δυνατότητα να συμπεράνουν ότι ένα συγκεκριμένο μήνυμα παρουσιάζει ενδιαφέρον για κάποιον, πόσο μάλλον να επιτελέσουν συγκεκριμένες πράξεις ώστε να μην περιέλθει το μήνυμα σε αυτόν. Εαν το λειτουργικό σύστημα ενός χρήστη καθιστά δυνατό μια διαδικασία να εμπλακεί σε μια άλλη διαδικασία, η Java δεν μπορεί να το αποτρέψει αυτό. Δεν μπορεί για παράδειγμα να αποτρέψει ένα χρήστη ο οποίος θα ξεγελαστεί εκτελώντας μια utilty η οποία συγκεντρώνει και στέλνει ένα E-mail με αυτά που "μαθαίνει". Οι περισσότεροι σήμερα υϊοθετούν τη boolean λογική, μιλώντας για ασφαλείς ή μη ασφαλείς τεχνολογίες. Όμως, υπάρχουν και άλλοι κρίκοι στην αλυσίδα που λέγεται "ασφάλεια ενός συστήματος"…

4.8 Μέλλον: η XML στη θέση της Java;

Με την τεράστια επέκταση του World Wide Web, πολλές εταιρίες δε δίστασαν να συνδεθούν στο δίκτυο παρέχοντας πληροφορίες για τις υπηρεσίες και τα προϊόντα τους. Η διατήρηση όμως ενημερωμένων και καλαίσθητων σελίδων αποδείχθηκε δύσκολη υπόθεση κυρίως λόγω της αναγκαστικής χρήσης της HyperText Markup Language. Ακόμα και με τη χρήση της Java η κατάσταση δεν καλυτέρευσε, αφού το πρόβλημα εντοπίζονταν στην ίδια τη δομή της HTML.

Η eXtensible Markup Language (XML) δημιουργήθηκε από το World Wide Web Consortium (W3C) για να άρει τους περιορισμούς που επέβαλε η HTML στη σχεδίαση σελίδων και κυρίως στην ανταλλαγή και αναζήτηση δεδομένων μέσω του Web. Είναι μια πολύ ευέλικτη γλώσσα που επιτρέπει τη διάθεση πιο περίπλοκων κειμένων και δεδομένων μέσω του Web.

Η XML αποτελεί έναν συμβιβασμό μεταξύ SGML και HTML, αφού κρατά την επεκτασιμότητα της πρώτης και την ευκολία και απλότητα της δεύτερης, μια και φτιάχτηκε για χρήση στον Web. Διαθέτει πολλά επιπλέον ισχυρά χαρακτηριστικά:

- Είναι μια ισχυρή και ευέλικτη γλώσσα μετάδοσης δεδομένων, είτε μεταξύ client/server εφαρμογών στο Internet, είτε μεταξύ προγραμμάτων που θα επεξεργάζονται αυτά τα δεδομένα.

- Προσφέρει έναν μηχανισμό προσθήκης meta-data ή meta-content στις HTML σελίδες.

- Δίνει μεγαλύτερες δυνατότητες στους Web authors, αφού επιτρέπει τη μετάβαση από ένα hyperlink σε περισσότερες σελίδες καθώς και την καλύτερη μορφοποίηση κειμένων μέσω αυστηρότερων εντολών (tags). Μια πολύ σημαντική δυνατότητα της XML είναι η δημιουργία νέων εντολών από το συγγραφέα μιας σελίδας, κάτι που δεν το επιτρέπει η HTML.

- Προσδίδει μεγαλύτερη ασφάλεια στις σελίδες, αφού μπορούν να προστεθούν μη

εμφανίσιμες ψηφιακές υπογραφές ή κρυπτογράφηση σε όλο το μέρος του κειμένου.

- Διαχωρίζει το περιεχόμενο από τον τρόπο παρουσίασης επιτρέποντας στις XML σελίδες να διαβάζονται από άλλες συσκευές εκτός από υπολογιστές όπως smart phones ή personal digital assistants.

Ασφάλεια Συστήματος 5

5.1 Ασφάλεια λειτουργικού συστήματος

Ένα λειτουργικό σύστημα (Λ.Σ) μεταξύ των άλλων πρέπει να παρέχει και λειτουργίες προστασίας των δεδομένων. Σε ένα υπολογιστικό σύστημα τα δεδομένα αποθηκεύονται ή επεξεργάζονται σε κάποιο υπολογιστικό πόρο (π.χ Αρχείο, Μνήμη, Συσκευή I/O). Η προστασία των δεδομένων αυτών σημαίνει έλεγχο ώστε μόνο οι εξουσιοδοτημένοι χρήστες να έχουν πρόσβαση στους πόρους αυτούς ή αντικείμενα (objects). Επομένως, πέρα των λειτουργιών υποστήριξης των βασικών υπηρεσιών ενός Λ.Σ, όπως εκτέλεση προγράμματος, διαχείριση αρχείων, διαχείριση I/O, κατανομή πόρων, μερικές από τις λειτουργίες του Λ.Σ είναι προσανατολισμένες αποκλειστικά στην παροχή υπηρεσιών ασφαλείας. Τέτοιες λειτουργίες είναι:

- Αυθεντικοποίηση (Authentication)
- Έλεγχος προσπέλασης (Access Control)
- Έλεγχος ροής (Flow control)
- Προστασία μνήμης (Memory protection)

5.1.1 Αναγνώριση ταυτότητας/Αυθεντικοποίηση

Οι μηχανισμοί αυθεντικοποίησης επαληθεύουν την ταυτότητα του χρήστη μέσω κάποιου αντικειμένου ή πληροφορίας γνωστής στο χρήστη, μέσω κάποιου στοιχείου που βρίσκεται στην κατοχή του χρήστη ή συνδυασμό αυτών. Συστήματα αυθεντικοποίησης που βασίζονται σε πληροφορίες γνωστές στο χρήστη είναι:

- Συστήματα χρήσης συνθηματικού (password)
- Συστήματα “ερώτημα-απάντηση” (query-answer)
- Συστήματα διπλής αυθεντικοποίησης (two-way authentication)

Στα **συστήματα χρήσης password**, η αναγνώριση της ταυτότητας του χρήστη πραγματοποιείται μέσω μιας μυστικής συμβολοσειράς γνωστής μόνο στο χρήστη και το σύστημα. Στα συστήματα πολλών χρηστών, τα passwords καταχωρούνται σε κάποιο αρχείο το οποίο διαχειρίζεται το Λ.Σ. Συνήθως προτιμάται η αποθήκευση των passwords σε μια περιοχή της μνήμης προσπελάσιμης μόνο από το Λ.Σ, όμως κάτι τέτοιο σημαίνει ότι όλα τα modules του Λ.Σ μπορούν να έχουν προσπέλαση στο αρχείο των passwords. Έτσι, μη εξουσιοδοτημένοι χρήστες εκμεταλλευόμενοι ειδικά modules του Λ.Σ, (trapdoors) θα μπορούσαν να προσπελάσουν το αρχείο. Ένα πρόσθετο μέτρο είναι η ύπαρξη ειδικών διαδικασιών login για πρσπέλαση στο αρχείο των passwords. Όμως, και σε αυτήν την περίπτωση, μη εξουσιοδοτημένοι χρήστες θα μπορούσαν να διαβάσουν όλη τη μνήμη και συνεπώς την περιοχή εκείνη που περιέχει το συγκεκριμένο αρχείο. Μειονεκτήματα της μορφής αυτής έχουν αντιμετωπιστεί με την κωδικοποίηση των passwords με τη χρήση κρυπτογραφικών αλγορίθμων. Δηλαδή, τα passwords κωδικοποιούνται και

καταχωρούνται στο αρχείο το οποίο μπορεί να διαβασθεί από όλους τους χρήστες, αλλά μόνο το Λ.Σ μπορεί να το τροποποιήσει (εισαγωγή, διαγραφή, ενημέρωση). Η προστασία του αρχείου επιτυγχάνεται με πολύπλοκους αλγόριθμους κρυπτογράφησης η αποκρυπτογράφηση των οποίων είναι σχεδόν αδύνατη.

Στα **συστήματα "ερώτημα-απάντηση"** ένας χρήστης αναγνωρίζεται μέσω μιας σειράς απαντήσεων σε ένα σύνολο ερωτημάτων που τίθενται από το Λ.Σ. Τα ερωτήματα είναι συγκεκριμένα για κάθε χρήστη και συνήθως βασίζονται σε μαθηματικές συναρτήσεις που υπολογίζονται από το σύστημα μετά την εισαγωγή τιμών από το χρήστη.

Στα **συστήματα διπλής αυθεντικοποίησης** (hand-shaking) το σύστημα αυθεντικοποιεί τον εαυτό του στο χρήστη εκτός από την αυθεντικοποίηση του χρήστη στο σύστημα. Η αυθεντικοποίηση του συστήματος πραγματοποιείται μέσω κάποιας πληροφορίας γνωστής μόνο στο χρήστη (π.χ ημερομηνία, χρόνος κωδικός).

Τα συστήματα αυθεντικοποίησης που βασίζονται σε πληροφορίες που κατέχει ο χρήστης είναι συνήθως συστήματα που χρησιμοποιούν κάποιο είδος κάρτας (π.χ magnetic, smart card). Η αυθεντικοποίηση πραγματοποιείται με την εισαγωγή της κάρτας σε σύστημα αναγνώστη-κάρτας και την πληκτρολόγηση κάποιου κωδικού. Μερικά από τα συστήματα αυτά είναι:

- Συστήματα δακτυλικού αποτυπώματος (fingerprint systems)
- Συστήματα φωτογραφίας χρήστη (facsimile systems)
- Συστήματα αναγνώρισης φωνής (voice recognition systems)
- Συστήματα με τη βοήθεια υπογραφής (hand-pressure systems)
- Συστήματα χαρακτηριστικών του αμφιβληστροειδούς (retinal features)

5.1.2 Έλεγχος προσπέλασης

Τα εκτελούμενα προγράμματα ή διεργασίες χρειάζονται υπολογιστικούς πόρους για την πραγματοποίηση των εργασιών τους. Γενικά, οι διεργασίες αναφέρονται σε διευθύνσεις μνήμης, χρησιμοποιούν την Κ.Μ.Ε (CPU), καλούν άλλα προγράμματα, χρησιμοποιούν τα αρχεία δεδομένων και προσπελαύνουν πληροφορίες στη δευτερεύουσα μνήμη (συσκευές I/O). Όλοι αυτοί οι υπολογιστικοί πόροι πρέπει να προσταεύονται από εσκεμμένη ή τυχαία μη εξουσιοδοτημένη χρήση.

Η προστασία της μνήμης και ο καταμερισμός ενός προγράμματος υλοποιείται άμεσα από το hardware το οποίο προστατεύει και την CPU. Η προστασία όλων των άλλων πόρων (αρχεία, συσκευές I/O) υλοποιείται μέσω μηχανισμών hardware και modules λογισμικού του Λ.Σ. Τα modules αυτά εκτελούν το ακόλουθο έργο:

- Αναλύουν και ελέγχουν κάθε ερώτημα προσπέλασης στους υπολογιστικούς πόρους (access control).
- Ελέγχουν τον προορισμό των εξερχομένων έτσι ώστε να προστατεύεται η διαρροή εμπιστευτικών δεδομένων (flow control).
- Παρακολουθούν και καταγράφουν τις εκτελούμενες λειτουργίες έτσι ώστε να εντοπίζεται κάθε μη εξουσιοδοτημένη χρήση των υπολογιστικών πόρων (audit)

5.1.3 Έλεγχος ροής

Οι μηχανισμοί ελέγχου ροής (flow control) είναι υπεύθυνοι για τον έλεγχο των δικαιωμάτων των χρηστών για προσπέλαση στους υπολογιστικούς πόρους, έτσι ώστε μόνο οι λειτουργίες που έχουν εγκριθεί να πραγματοποιούνται. Μέσω των

μηχανισμών αυτών πραγματοποιείται η επαλήθευση του τελικού προορισμού των εξερχομένων μιας λειτουργίας ώστε να αποφεύγεται η διάδοση των πληροφοριών.

Μια ροή πραγματοποιείται όταν οι πληροφορίες μετακινούνται από ένα αντικείμενο-πηγή σε ένα αντικείμενο-προορισμό. Γενικά, υπάρχουν δύο είδη ροής: άμεση ή εσωτερική (explicit) και υπό συνθήκη ή εξωτερική (implicit). Η πρώτη πραγματοποιείται ως αποτέλεσμα εντολών μεταβίβασης, ενώ η δεύτερη προκύπτει από εντολές συνθήκης.

Οι μηχανισμοί ελέγχου ροής υλοποιούν τον έλεγχο με τον ορισμό μιας ετικέτας διαβάθμισης σε κάθε αντικείμενο, η οποία προσδιορίζει την κλάση ασφαλείας του αντικειμένου. Στη συνέχεια, οι ετικέτες χρησιμοποιούνται για την επαλήθευση των σχέσεων ροής που ορίζονται στο αντίστοιχο μοντέλο.

5.1.4 Προστασία μνήμης

Σε περιβάλλοντα πολυπρογραμματισμού, η κύρια μνήμη του συστήματος χωρίζεται και αποδίδεται στα προγράμματα και τα δεδομένα των χρηστών. Το γεγονός αυτό συνεπάγεται την προστασία της μνήμης και των προγραμμάτων από αμοιβαία αλληλεπικοινωνία. Επιπλέον, οι ίδιοι υπολογιστικοί πόροι χρειάζεται να διαμοιράζονται μεταξύ διαφορετικών χρηστών. Κατά συνέπεια, υπάρχουν διάφορα επίπεδα διαμοίρασης τα οποία εκτείνονται από την πλήρη απομόνωση (no sharing) έως τη μη ελεγχόμενη διαμοίραση (uncontrolled sharing). Ενδιάμεσα επίπεδα διαμοίρασης μπορούν να επιλεγούν, όπως αυτό της διαμοίρασης αντιγράφων των αντικειμένων (sharing of copies), όπου οι χρήστες εργάζονται με τα δικά τους αντίγραφα ενώ το κύριο (master) αντίγραφο ενημερώνεται περιοδικά, και αυτό της διαμοίρασης των πρωτότυπων αντικειμένων (sharing of original objects) όπου ένα μοναδικό αντίγραφο ενός αντικειμένου διατίθεται σε όλους τους χρήστες. Συνήθως, η διαμοίραση περιλαμβάνει τα πρωτότυπα των δεδομένων και των προγραμμάτων για εξοικονόμηση χώρου και χρόνου ενώ με ένα μοναδικό αντίγραφο η κατάσταση του αντικειμένου είναι πάντοτε ενημερωμένη και συνεπής.

Η υλοποίηση ενός μηχανισμού ελεγχόμενης διαμοίρασης απαιτεί προστασία σε επίπεδο Λ.Σ για τη διαχείριση ζητημάτων που σχετίζονται με:

- Ταυτόχρονη προσπέλαση (concurent access), δηλαδή ερωτήματα προσπέλασης για το ίδιο αντικείμενο, από διαφορετικούς χρήστες σε διαφορετικό χρόνο.
- Περιορισμένη προσπέλαση (confinement). Ισχύει μόνο για προγράμματα και αφορά την απαγόρευση αντιγραφής των παραμέτρων τους. Έτσι, ένα πρόγραμμα διαμοίρασης παρεμποδίζεται στο να αντιγράφει και να μεταφέρει δεδομένα εισόδου σε αρχεία του συστήματος.

Οι διάφοροι μέθοδοι για την προστασία και τον έλεγχο της διαμοιραζόμενης μνήμης είναι οι ακόλουθοι:

- Μέθοδος φραγμού (fence address)
- Μέθοδος αναδιεύθυνσης (relocation)
- Μέθοδος καταχωρητή (base/bound)
- Μέθοδος σελιδοποίησης (paging)
- Μέθοδος τμηματοποίησης (segmentation)

5.2 Intrusion Detection Systems (IDS)

Ένα *Σύστημα Ανίχνευσης Εισβολής* ή IDS εν συντομία, επιχειρεί να ανιχνεύσει έναν "κακόβουλο" χρήστη που εισβάλλει στο σύστημα, ή έναν νόμιμο

χρήστη που προσπαθεί να εκμεταλλευθεί με κακό σκοπό τους πόρους του συστήματος. Ένα IDS εκτελείται μόνιμα στο σύστημα, συγκεκριμένα στο background, προειδοποιώντας τον administrator του συστήματος σε περίπτωση που ανιχνεύσει μια ύποπτη λειτουργία.

Υπάρχουν δύο κατηγορίες δυνητικών εισβολέων:

- **Έξωθεν εισβολείς (outside):** Οι περισσότεροι υπεύθυνοι συστημάτων σήμερα, θεωρούν την κατηγορία αυτή των εισβολέων ως τη μεγαλύτερη απειλή για την ασφάλεια των συστημάτων τους.

- **Έσωθεν εισβολείς (inside):** Μελέτες για λογαριασμό του FBI απέδειξαν ότι το 80% των εισβολών και των επιθέσεων προέρχονται από το εσωτερικό των επιχειρήσεων. Αυτό άλλωστε είναι κάτι φυσιολογικό, αφού οι έσωθεν γνωρίζουν καλύτερα από τον καθένα τη δομή των συστημάτων, ποιά και πόσα είναι τα πολύτιμα δεδομένα όπως και τους τρόπους που επιλέγονται για την προστασία τους.

Ένα υπολογιστικό σύστημα μπορεί να θεωρηθεί ως ένα σύνολο πόρων (resources) που είναι διαθέσιμοι στους εξουσιοδοτημένους χρήστες. Υπάρχουν έξι στοιχεία στην ασφάλεια ενός συστήματος, που πρέπει να αποτελούν και το βασικό στόχο:

1) **Διαθεσιμότητα** -το σύστημα, όπως και ορισμένα κρίσιμα δεδομένα πρέπει να είναι διαθέσιμα για χρήση, όποτε οι νόμιμοι χρήστες τα χρειάζονται.
2) **Χρησιμότητα** -το σύστημα, και τα δεδομένα στο σύστημα, πρέπει να είναι χρήσιμα σε κάτι.
3) **Ακεραιότητα** -το σύστημα και τα δεδομένα του πρέπει να είναι πλήρη και σε αναγνώσιμη μορφή.
4) **Αυθεντικοποίηση** - το σύστημα πρέπει να είναι ικανό να πιστοποιήσει την ταυτότητα χρηστών και οι χρήστες θα πρέπει να μπορούν να πιστοποιήσουν την ασφάλεια του συστήματος.
5) **Εμπιστευτικότητα** - τα εμπιστευτικά δεδομένα πρέπει να είναι γνωστά μόνον στον ιδιοκτήτη των δεδομένων, ή σε οποιονδήποτε αυτός επιλέξει.
6) **Κατοχή** - οι ιδιοκτήτες του συστήματος πρέπει να μπορούν να το ελέγξουν.Εαν ο έλεγχος του συστήματος περιέλθει σε έναν "κακόβουλο" χρήστη, αυτομάτως επηρρεάζονται όλοι οι χρήστες που σχετίζονται με το σύστημα.

Οι εισβολές καθ'αυτές, μπορούν να ταξινομηθούν σε δύο κατηγορίες:

- **Εκμετάλλευσης** (misuse), που είναι καλά ορισμένες επιθέσεις σε αδύναμα σημεία ενός συστήματος. Μπορούν να ανιχνευθούν με την εξέταση εάν έχουν πραγματοποιηθεί συγκεκριμένες πράξεις σε συγκεκριμένα αντικείμενα του συστήματος. Οι εισβολές αυτές ακολουθούν γνωστά μοντέλα επομένως ο συστηματικός έλεγχος των log αρχείων μπορεί να οδηγήσει εύκολα στην ανίχνευσή τους.
- **Ανομαλίας** (anomaly), που συνίστανται απλά σε παρεκκλίσεις από τη συνήθη λειτουργία του συστήματος. Ανιχνεύονται με τη δημιουργία ενός profile του συστήματος το οποίο ελέγχεται, και κατόπιν ελέγχοντας το αν και κατά πόσον υπάρχουν παρεκκλίσεις από αυτό το profile. Οι εισβολές αυτές είναι δύσκολο να ανιχνευτούν. Δεν υπάρχουν σταθερά μοντέλα που να μπορούν να χρησιμοποιηθούν με βεβαιότητα ως σημεία αναφοράς. Έτσι, τα IDS πρέπει να να υϊοθετούν μια "ασαφή" λογική στην προσέγγιση των εισβολών αυτού του είδους.

Πολλά IDS βασίζουν τη λειτουργία τους στην ανάλυση των ελέγχων ορθότητας του λειτουργικού συστήματος. Ένα IDS μπορεί επίσης να ασκεί τον δικό του έλεγχο του συστήματος, συσγκεντρώνοντας καταρχήν ένα σύνολο στατιστικών που καταγράφουν το profile της χρήσης του συστήματος. Τα στατιστικά αυτά στοιχεία μπορούν να εξαχθούν από μια ποικιλία πηγών, όπως η χρήση της CPU, των συσκευών I/O, της μνήμης, οι δραστηριότητες των χρηστών, ο αριθμός των logins, κ.λ.π. Αυτά τα στατιστικά πρέπει να ενημερώνονται συνεχώς ώστε να αντανακλούν τη τρέχουσα κατάσταση του συστήματος.

Ενα Σύστημα Ανίχνευσης Εισβολής (IDS) πρέπει να ανταποκρίνεται στις ακόλουθες απαιτήσεις, ανεξάρτητα από το μηχανισμό στον οποίο βασίζεται:

1. Πρέπει να **εκτελείται συνεχώς** χωρίς ανθρώπινη επιτήρηση. Το σύστημα πρέπει να είναι αρκετά αξιόπιστο ώστε να του επιτρέπεται η εκτέλεση στο background. Εντούτοις, δεν πρέπει να είναι ένα "black box": οι εσωτερικές του λειτουργίες πρέπει να επιδέχονται εξέτασης από τους "έξω".
2. Πρέπει να είναι **ανθεκτικό** υπό την έννοια ότι θα πρέπει να αντεπεξέλθει έπειτα από μια π.χ κατάρρευση του συστήματος, χωρίς να χρειάζεται να ξανα-χτίσει την βάση γνώσης του.
3. Πρέπει να **αυτοελέγχεται**, δηλαδή να ελέγχει τις λειτουργίες του, για την περίπτωση που έχει παραβιαστεί από κάποιον.
4. Πρέπει να επιβαρύνει το σύστημα με το **ελάχιστο φόρτο**. Ένα IDS που καταναλώνει μεγάλες ποσότητες υπολογιστικών πόρων, ζημιώνει περισσότερο από ό,τι προσφέρει.
5. Πρέπει να είναι **προσαρμόσιμο** στις ανάγκες του συστήματος στο οποίο χρησιμοποιείται. Κάθε σύστημα έχει ένα διαφορετικό μοντέλο χρήσης, οπότε και οι μηχανισμοί άμυνας πρέπει να προσαρμόζονται σε αυτά τα μοντάλα.
6. Δεν πρέπει να "ξεγελιέται" εύκολα.

Η τελευταία απαίτηση σχετίζεται άμεσα με τους τύπους των λαθών που μπορεί να συμβούν στη λειτρουργία του IDS. Τα λάθη αυτά, διακρίνονται σε **ψευδή θετικά** (false positive) και **ψευδή αρνητικά** (false negative). Ένα *ψευδές θετικό*, συμβαίνει όταν το σύστημα χαρακτηρίζει μια πράξη ως ανώμαλη (μια πιθανή εισβολή), ενώ είναι μια καθόλα νόμιμη πράξη. Ένα *ψευδές αρνητικό*, συμβαίνει όταν έχει πραγματοποιηθεί μια πράξη εισβολής, αλλά το σύστημα επιτρέπει την εξέλιξή της θεωρώντας την νόμιμη. Τα *ψευδή αρνητικά* λάθη είναι τα περισσότερο σοβαρά, καθώς συνήθως δημιουργούν ψευδαίσθηση ασφάλειας.

Τέλος, ανάλογα με το από πού προέρχονται τα δεδομένα που τα IDS επεξεργάζονται, μπορούμε να τα ταξινομήσουμε στις ακόλουθες τρεις κατηγορίες:

- **host-based,** όπου για την ανίχνευση εισβολών χρησιμοποιούνται δεδομένα ελέγχων ορθότητας ενός και μόνου host
- **multihost-based,** όπου χρησιμοποιούνται δεδομένα ελέγχων ορθότητας πολλών hosts
- **network-based,** χρησιμοποιούνται δεδομένα από την κίνηση στο δίκτυο (network traffic) σε συνδυασμό με δεδομένα ελέγχων ορθότητας από τους hosts του δικτύου.

5.3 Ασφάλεια Web Server

Υπάρχουν κάποια βήματα που πρέπει να ακολουθούνται από τους Web administrators, ώστε ο server να εκτελείται ασφαλώς χωρίς να θέτει σε κίνδυνο εμπιστευτικά αρχεία, άλλα προγράμματα, και τους χρήστες γενικότερα.

Δικαιώματα (file permissions)

Για μέγιστη ασφάλεια, πρέπει να εφαρμόζεται μια "αυστηρή" πολιτική όσον αφορά τα δικαιώματα των χρηστών στο document root (εκεί που αποθηκεύοται τα HTML έγγραφα) και στο server root (όπου φυλάσσονται τα αρχεία διαμόρφωσης- configuration και καταγραφής-log) .

Μια απλή στρατηγική είναι η δημιουργία ενός "www" χρήστη για τη διαχείριση (webmaster) και μιας "www" ομάδας (group) για όλους τους χρήστες του συστήματος που επιθυμούν να συγγράψουν HTML έγγραφα. Σε ένα Unix σύστημα, χρειάζονται αλλαγές στο αρχείο /etc/passwd ώστε το server root να γίνει το home directory για τον χρήστη www. Επίσης, χρειάζονται αλλαγές στο αρχείο /etc/group ώστε να προστεθούν οι συγγραφείς HTML εγγράφων στην ομάδα www.

Το **server root** πρέπει να διαμορφωθεί ώστε μόνον ο χρήστης www να μπορεί να γράψει στους καταλόγους των αρχείων διαμόρφωσης και καταγραφής, αλλά και στα περιεχόμενά τους. Έγκειται στον διαχειριστή να αποφασίσει εαν οι κατάλογοι αυτοί πρέπει να είναι αναγνώσιμοι από την ομάδα www. Το σίγουρο είναι ότι δεν πρέπει να είναι αναγνώσιμοι από όλους (world-readable). Ο κατάλογος cgi-bin και τα περιεχόμενά του πρέπει να είναι εκτελέσιμα και αναγνώσιμα από όλους, αλλά όχι εγγράψιμα.

Το **document root** χρειάζεται διαφορετική αντιμετώπιση. Όλα τα αρχεία που εξυπηρετούν (server) στο Internet πρέπει να είναι αναγνώσιμα από τον server, ενώ αυτός θα εκτελείται με τα δικαιώματα του χρήστη "nobody". Επίσης, οι τοπικοί Web authors θα πρέπει να μπορούν να προσθέσουν αρχεία στο document root. Επομένως, ο κατάλογος document root και οι υποκατάλογοί του θα ανήκουν στον χρήστη και στην ομάδα "www", θα είναι αναγνώσιμα από όλους (world readable) και εγγράψιμα από την ομάδα (group writable).

Εκτέλεση του server (running the server)

Καθημερινά εγείρονται πολλές διαφωνίες στο Internet σχετικά με την ταυτότητα χρήστη υπό την οποία πρέπει να εκτελείται ο Web server. Οι περισσότεροι servers εκτελούνται ως root ώστε να μπορούν να "ανοίξουν" την port 80 (η standard HTTP port) και να γράψουν στα log αρχεία. Στη συνέχεια, αναμένουν για μια εισερχόμενη σύνδεση στην port 80. Μόλις λάβουν τη σύνδεση, "εξ-ωθούν" (fork) μια υπο-διαδικασία (child process) να αναλάβει την αίτηση, και επιστρέφουν σε κατάσταση αναμονής. Η υπο- διαδικασία αυτή εντωμεταξύ, μεταβάλλει το ID χρήστη της σε αυτό του χρήστη "nobody" και κατόπιν χειρίζεται την αίτηση. Όλες οι ενέργειες που γίνονται ως απάντηση στις αιτήσεις του απομακρυσμένου χρήστη, όπως η εκτέλεση CGI scripts ή Server-Side Includes, γίνονται με τα δικαιώματα του χρήστη "nobody" (μη προνομιούχος χρήστης).

Ο κίνδυνος υφίσταται, όχι τόσο όταν ο server εκτελείται ως root, αλλά όταν ο server έχει διαμορφωθεί ώστε η υπο-διαδικασία να εκτελείται με δικαιώματα root (καθορίζοντας "User root" στο αρχείο διαμόρφωσης του server). Εαν συμβαίνει κάτι τέτοιο, τότε π.χ κάθε CGI script θα έχει δικαιώματα root, με καταστροφικά αποτελέσματα.

Ορισμένοι υποστηρίζουν πως δεν πρέπει ούτως ή άλλως να εκτελείται ο server ως root. Θεωρούν πως είναι δύσκολο να ελέγξει κανείς απόλυτα τη συμπεριφορά του server από τη στιγμή που αρχικοποιείται εως τη στιγμή που θα "εξ-ωθήσει" (fork) την υπο- διαδικασία, και πως οι servers συχνά έχουν λάθη στον κώδικα λειτουργίας τους. Έτσι, πολλά sites αρχικοποιούν τον server ως τον χρήστη "nobody", "daemon" ή "www". Βέβαια, σε αυτήν την περίπτωση, πρέπει να ληφθούν υπ'όψην τα ακόλουθα:

1. Ο server δε θα είναι ικανός να ανοίξει τη port 80. Θα πρέπει να διαμορφωθεί ώστε να "ακούει" σε άλλη port, όπως η 8000 ή 8080.
2. Τα αρχεία διαμόρφωσης (configuration files) πρέπει να είναι αναγνώσιμα από το ίδιο ID με το οποίο εκτελείται ο server. Κάτι τέτοιο αφήνει ανοιχτό το ενδεχόμενο ένα CGI script να μπορεί να διαβάσει τα αρχεία διαμόρφωσης. Ομοίως, τα log αρχεία πρέπει να αναγνώσιμα και εγγράψιμα από το ID αυτό, με αποτέλεσμα ένα παραβιασμένο CGI script να μπορεί να αλλάξει το log.

Web και ftp Servers

Πολλά sites αρέσκονται στο να διατηρούν το ίδιο "δένδρο εγγράφων" (document tree) τόσο για τον Web όσο και για τον FTP server. Αυτό δεν συνιστά απαραίτητα "τρύπα" ασφαλείας, αρκεί να μην υπάρχει τρόπος ένας χρήστης να κάνει upload αρχεία τα οποία αργότερα θα μπορέσει να αναγνώσει ή εκτελέσει με τον Web daemon.

Άλλες προτεραιότητες

Τέλος, ολοκληρώνοντας, υπάρχουν και ορισμένες άλλες ενέργειες (όχι λιγότερο σημαντικές) που πρέπει να γίνουν ώστε ο server να είναι σχετικά ασφαλής:

- Πρέπει να καθοριστεί μια συγκεκριμένη πολιτική ασφαλείας, η οποία πρέπει να ακολουθείται πιστά.
- Φιλτράρισμα πακέτων στα πλαίσια ενός firewall ή ενός δρομολογητή που έχει δυνατότητες φιλτραρίσματος.
- Τα εργαλέια software και οι τεχνικές που χρησιμοποιούνται για την ασφάλεια του συστήματος πρέπει να είναι τελευταίας έκδοσης (version).
- Συνεχής εκπαίδευση των Web administrators αλλά και των χρηστών που χρησιμοποιούν τον server.
- Καθημερινοί έλεγχοι ορθότητας (auditing) και περιοδικοί έλεγχοι για αδυναμίες του συστήματος.
- Σύσταση μιας λίστας hosts, στους οποίους θα επιτρέπεται η πρόσβαση σε εμπιστευτικά έγγραφα .
- Απενεργοποίηση όλων εκείνων των εφαρμογών που δε χρησιμοποιούνται από τον server.
- Προστασία όλων των υπηρεσιών που παρέχονται από το σύστημα που "φιλοξενεί" τον server (smtp, ftp κ.λ.π).
- Απενεργοποίηση των Server Side Includes.
- Χρήση ασφαλών πρωτοκόλλων για την επικοινωνία με το υπόλοιπο Internet (shttp, PCT, SSL, κ.λ.π).
- Έλεγχος των δεδομένων που εισάγουν απομακρυσμένοι χρήστες στα πεδία μιας HTML φόρμας, ώστε να ανιχνεύονται "κακόβουλα" δεδομένα (π.χ shell μετα- χαρακτήρες).

Ασφάλεια και Web Search Engines

Σήμερα οι μηχανές αναζήτησης (π.χ Yahoo, Google) έχουν γίνει περισσότερο ισχυρές από ποτέ . Ορισμένα Web sites παρέχουν πολλά links, συμπεριλαμβανομένων και πληροφοριών που αφορούν τις ρυθμίσεις του συστήματος. Για παράδειγμα, εαν κάποιος κάνει μια έρευνα με μια από αυτές τις μηχανές αναζήτησης, με λέξεις κλειδί 'root', 'daemon', 'passwd', κ.λ.π, τότε η μηχανή αναζήτησης ενδεχομένως να εμφανίσει μια λίστα από αρχεία /etc/passwd ή /etc/group, τα οποία βρίσκονται σε συστήματα με "αδύναμες" ρυθμίσεις και μηχανισμούς ασφαλείας. Έτσι, αυτός είναι ένας γρήγορος

τρόπος να ανακαλυφθούν τα ευάλωτα συστήματα στο Internet.

Οι Web administrators πρέπει να είναι προσεκτικοί σχετικά με το τί είδους πληροφορία είναι διαθέσιμη στο Internet, ενώ δεν πρέπει να υπάρχουν URLs που οδηγούν σε εμπιστευτικές πληροφορίες.

5.4 Ασφάλεια anonymous FTP Server

Το File Transfer Protocol, ή FTP, αποτελεί τη βάση για τον αρχαιότερο τύπο υπηρεσίας στο Internet, τον anonymous FTP server . Οι anonymous FTP servers επιτρέπουν μη εξουσιοδοτημένη πρόσβαση σε ένα τμήμα του συστήματος αρχείων (file system) του host. Το software του server επιτρέπει σε απομακρυσμένους χρήστες να ανακτούν αρχεία, περιστασιακά να "ανεβάζουν" (upload) αρχεία, ή ακόμα και πιο προηγμένες λειτουργίες όπως συμπίεση αρχείων.

Αδυναμίες του anonymous FTP Server

Οι anonymous FTP servers έχουν ορισμένα "τρωτά" σημεία. Αυτά είναι τα εξής:

- Χρήστες στο Internet ενδέχεται να χρησιμοποιούν εγγράψιμες περιοχές στο FTP σύστημα αρχείων ώστε να ανταλλάσουν αρχεία. Αυτή είναι μια συνήθης τεχνική για ανταλλαγή παράνομου ή copyrighted software, καθώς και πορνογραφικών εικόνων.
- Οι χρήστες μπορούν να αλλάξουν/σβήσουν πληροφορίες ή software.
- Στο παρελθόν, ανακαλύφθησαν αδυναμίες στο FTP software, οι οποίες επέτρεπαν πλήρη πρόσβαση στα αρχεία του συστήματος . Αυτές οι αδυναμίες εξαλείφθησαν αλλά καθώς προστίθενται συνεχώς καινούρια χαρακτηριστικά στο software, είναι πιθανή η εμφάνιση άλλων αδυναμιών.
- Λάθη στις ρυθμίσεις (configuration errorrs) ενδέχεται να επιτρέπουν πρόσβαση σε εμπιστευτικά αρχεία. Για παράδειγμα, ένα σύνηθες λάθος στη διαμόρφωση του anonymous FTP server είναι όταν ένα αντίγραφο του αρχείου passwords του συστήματος τοποθετείται σε περιοχή διαθέσιμη στους απομακρυσμένους χρήστες. Εαν οι τοπικοί χρήστες έχουν επιλέξει "αδύναμα" passwords, οι εισβολείς μπορούν να χρησιμοποιήσουν το αρχείο passwords ώστε να παραβιάσουν το σύστημα.

Ρυθμίσεις του anonymous FTP Server

Υπάρχουν ορισμένοι κανόνες που πρέπει να ακολουθούνται στη ρύθμιση ενός anonymous FTP server:

- Δεν πρέπει να υπάρχουν αρχεία ή κατάλογοι στην anonymous FTP περιοχή (area), που να ανήκουν στον χρήστη 'ftp'. Αυτό είναι το ID των anonymous χρηστών, και ο,τιδήποτε ανήκει σε αυτό το ID μπορεί να τροποποιηθεί να αντικατασταθεί, ή να σβηστεί από κάποιον απομακρυσμένο χρήστη στο Internet.
- Δεν πρέπει να υπάρχουν κρυπτογραφημένα passwords από το αρχείο passwords του συστήματος (/etc/passwd) στο αρχείο passwords της anonymous FTP περιοχής (~ftp/etc/passwd). Οποιοσδήποτε από το Internet θα μπορούσε να αποκτήσει τα κρυπτογραφημένα αυτά passwords, και να προσπαθήσει να τα αποκρυπτογραφήσει.
- Εαν είναι δυνατόν, δε θα πρέπει να επιτρέπεται εγγραφή σε αρχεία ή καταλόγους από anonymous χρήστες.

5.5 Ασφάλεια Browser

Για τους περισσότερους, το Internet είναι ο νοητός εκείνος χώρος όπου εκτελούν κυρίως αυτό που ονομάστηκε "surfing". Ένα από τα σημαντικά πεδία

ανταγωνισμού των επίδοξων κηδεμόνων του χώρου, αποτέλεσε και αποτελεί το λογισμικό που χρησιμοποιείται για το σκοπό αυτό, δηλαδή οι Web browsers. Η εξέλιξή τους συνδέεται με όλες τις εκάστοτε τάσεις και τεχνολογίες που προτείνονται όπως η Java, το ActiveX, το scripting και πολλά άλλα. Είναι αλήθεια ότι η συγγραφή σελίδων html, δεν είναι πια η απλή υπόθεση πρόσθεσης ετικετών σε κάποιο κείμενο text, αλλά αποτελεί ειδική περίπτωση ανάπτυξης λογισμικού. Το λογισμικό αυτό δύναται να τρέχει στον αναγνώστη των σελίδων (client), και κατά συνέπεια να παρεμβαίνει στο σύστημά του. Θεωρητικά, το επίπεδο της παρέμβασης αυτής καθορίζεται από τη σχεδίαση των χρησιμοποιούμενων πρωτοκόλλων και την υλοποίησή τους στους browsers. Πρακτικά, φαίνεται ότι πολλές παράμετροι δεν έχουν ληφθεί υπόψην ως όφειλαν, με αποτέλεσμα το περιθώριο παρέμβασης να είναι ιδιαίτερα μεγάλο, δημιουργώντας προβλήματα ασφαλείας και ερωτηματικά στους χρήστες.

Στο κεφάλαιο 4 αναφερθήκαμε διεξοδικά για ορισμένες παραβιάσεις ασφαλείας που σχετίζονταν με αδυναμίες των δημοφιλών Web browsers στην ενσωμάτωση της Java τεχνολογίας. Τα λάθη αυτά είναι χαρακτηριστικά των αδυναμιών που παρουσιάζουν οι browsers που διατίθενται στο Web. Εδώ, θα παρουσιάσουμε ενδεικτικά μία ακόμη παραβιάση, που δεν αφορά τη Java, αλλά είναι εξίσου χαρακτηριστική:

- Τον Απρίλιο 1997, ανακαλύφθηκε ένα σοβαρό πρόβλημα του **Internet Explorer 3.01** το οποίο επιτρέπει στους συγγραφείς σελίδων web να χρησιμοποιήσουν αρχεία τύπου .URL και .LNK για να τρέξουν προγράμματα στον υπολογιστή του αναγνώστη (client), με όλες τις συνεπακόλουθες δυνατές συνέπειες. Μάλιστα, η περίπτωση των αρχείων .URL είναι πιο επικίνδυνη, διότι τα αρχεία αυτά τρέχουν και σε Windows NT. Επίσης, τα client side scripts μπορούν να χρησιμοποιήσουν το αντικείμενο 'Explorer' για να μεταφέρουν ένα αρχείο batch στον υπολογιστή του χρήστη και στη συνέχεια να το εκτελέσουν.

Ο **Internet Explorer**, που περιλαμβάνεται στα Windows 95, υποστηρίζει τις τεχνολογίες SSL, PCT (Private Communication Technology) και SET (Secure Electronic Transaction) για αυθεντικοποίηση, ακεραιότητα και εμπιστευτικότητα στο Web. Επίσης, υποστηρίζει την τεχνολογία Authenticode για ασφαλή παροχή πιστοποιητικών σε συναλλαγές. Ο Internet Explorer προειδοποιεί τους χρήστες του σε περίπτωση ύπαρξης μιας μη ασφαλής σύνδεσης, ενώ όταν η σύνδεση είναι ασφαλής εμφανίζει ένα χαρακτηριστικό icon στο status line. Επιτρέπει στους χρήστες να καθορίσουν μόνοι τους το επίπεδο ασφάλειας και τον τρόπο προειδοποίησής τους. Τέλος, υποστηρίζει την τεχνολογία S/MIME για ανταλλαγή e-mail.

Ο **HotJava browser** ενσωματώνει πλήρως την τεχνολογία της Java. Έχει τη δυνατότητα να προσαρμόζεται γρήγορα σε καινούρια πρωτόκολλα, χωρίς να περιορίζεται σε συγκεκριμένες λειτουργίες. Λειτουργεί ως ένας "έξυπνος" interpreter εκτελέσιμου περιεχομένου, ικανός να εμφανίζει καινούρια formats. Ο Hotjava κληρονομεί τα χαρακτηριστικά ασφαλείας της Java, όπως περιορισμό πρόσβασης στη μνήμη, πιστοποίηση bytecodes και Security Manager . Έχει δυνατότητα χρήσης κρυπτογραφικών μηχανισμών δημόσιου κλειδιού, ενώ μπορεί να διακρίνει εαν το bytecode προέρχεται μέσα ή έξω από το firewall.

Αρμοδιότητες των χρηστών

Παρά το γεγονός ότι, αν υπάρχει ένα λάθος στον κώδικα του browser τότε οι χρήστες είναι σχετικά "απροστάτευτοι", υπάρχουν ορισμένα μέτρα πρόληψης:

1) Οι χρήστες πρέπει να κάνουν συχνά backup στα εμπιστευτικά τους αρχεία. Οι σύγχρονοι δίσκοι δε χαλάνε εύκολα, αλλά είναι ευάλωτοι από άλλες πλευρές.

2) Οι χρήστες πρέπει να "μοιράζουν" στο δίκτυο μόνο ότι είναι εντελώς απαραίτητο, και για όσο λιγότερο χρόνο γίνεται. Τα σημαντικά αρχεία πρέπει να κρατούνται όσο γίνεται μακριά από (ακόμα και φυσική, αν είναι δυνατόν) προσπέλαση τρίτων.

3) Πρέπει να αγνοούνται οι προτεινόμενες τοποθεσίες εγκατάστασης προγραμμάτων. Τα 'C:\My documents' και 'C:\Windows' είναι πολύ ανυποψίαστες επιλογές, άμεσα αντιληπτές.

4) Πλήρης αξιοποίηση των επιλογών ασφαλείας σχετικά με Java και Activex applets, που παρέχονται στο παραθυρικό περιβάλλον του εκάστοτε browser.

5) Απόκτηση της πιο πρόσφατης έκδοσης (version) του browser, η ανακοίνωση της οποίας οφείλεται συνήθως σε λάθη της προηγούμενης.

5.5.1 Web Spoofing

Το Web spoofing είναι μία επίθεση που δέχονται οι χρήστες των περισσότερο δημοφιλών σήμερα Web browsers που απειλεί την ασφάλεια των πολύτιμων δεδομένων τους καθώς και των συναλλαγών στις οποίες επιδίδονται καθημερινά . Το Web spoofing, συνίσταται στην δημιουργία, από κάποιον δολιοφθορέα, ενός ολόκληρου αντίγραφου του World Wide Web. Οι προσβάσεις σε αυτό το "ψεύτικο" Web επιτυγχάνονται διαμέσου της μηχανής του δολιοφθορέα, επιτρέποντας σε αυτόν να ελέγχει και να παρακολουθεί όλες τις κινήσεις του θύματος, συμπεριλαμβανομένων passwords ή αριθμών λογαριασμών που το θύμα πληκτρολογεί. Ο δολιοφθορέας μπορεί επίσης να στείλει ψεύτικα δεδομένα σε Web servers για λογαριασμό του χρήστη, ή στο θύμα για λογαριασμό οποιουδήποτε Web server. Με άλλα λόγια, ελέγχει οτιδήποτε κάνει ο χρήστης-θύμα στο Web.

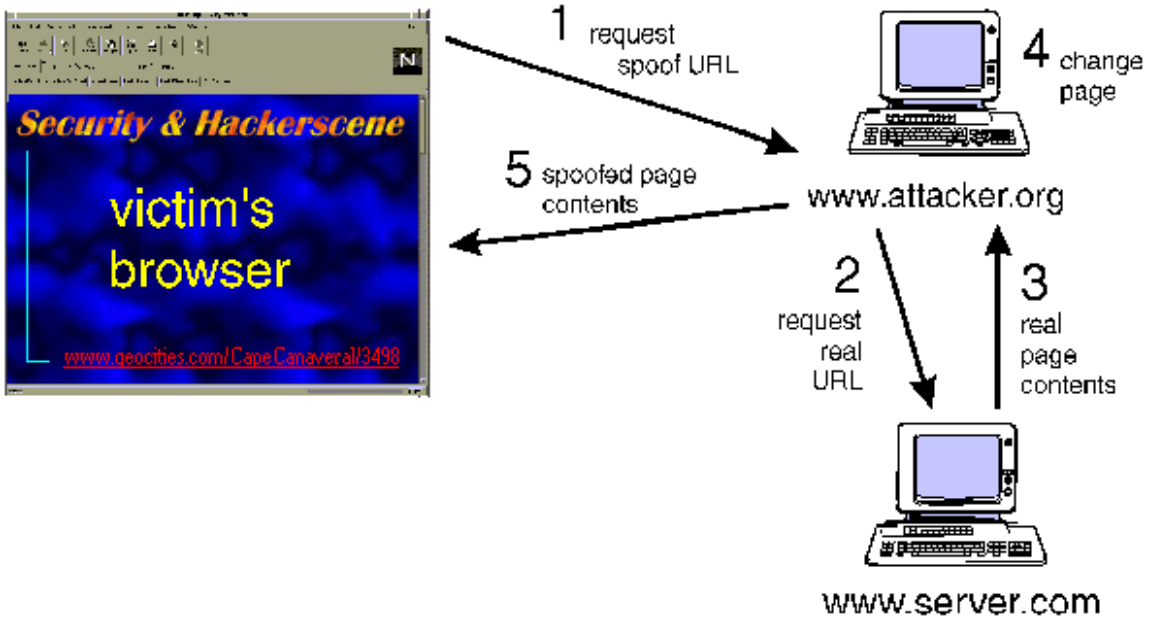
Με το Web spoofing, ο "κακός" έχει τη δυνατότητα και να παρατηρήσει τις κινήσεις του χρήστη, αλλά και να επέμβει στις επιλογές του (του χρήστη), όπως είδαμε παραπάνω. Μπορεί δηλαδή να παρατηρεί παθητικά την πλοήγηση του χρήστη, καταγράφοντας ποιές σελίδες αυτός συνηθίζει να επισκέπτεται. Όταν ο χρήστης συμπληρώνει μια φόρμα, τα εισηγμένα δεδομένα κατευθύνονται προς ένα Web server, οπότε ο "κακός" μπορεί να τα καταγράψει και αυτά επίσης, όπως επίσης μπορεί και να καταγράψει και τις απαντήσεις του server. Όπως θα δούμε παρακάτω, ο "κακός" μπορεί να παρατηρεί τις κινήσεις του χρήστη, ακόμα και εαν ο χρήστης-θύμα έχει μια "ασφαλή" σύνδεση (συνήθως μέσω του SSL) με ένα server, δηλαδή ακόμα και αν ο browser του χρήστη δείχνει το εικονίδιο ασφαλής σύνδεσης στο αριστερό τμήμα της status bar του browser που χρησιμοποιεί.

Επίσης, ο "κακός" μπορεί να τροποποιήσει δεδομένα που εισάγει ο χρήστης, π.χ όταν παραγγέλνει online ένα προιόν. Ο "κακός" μπορεί να αλλάξει τον κωδικό του προιόντος, την ζητούμενη ποσότητα, τη διεύθυνση παραλαβής. Μπορεί επίσης να τροποποιήσει τα δεδομένα που κατευθύνονται από το server προς το χρήστη, π.χ στέλνοντας εκ μέρους του server μηνύματα προσβλητικού περιεχομένου προς το χρήστη, δημιουργώντας έτσι ένα κλίμα αντιπαλότητας μεταξύ του server και του χρήστη. Ίσως ακούγεται παράξενο το ότι κάποιος μπορεί να "εξομοιώσει¨ολόκληρο το World Wide web, αλλά δεν είναι. Ο "κακός" δεν χρειάζεται να αποθηκεύσει κάπου ολόκληρο το περιεχόμενο του Web. Ολόκληρο το Web είναι διαθέσιμο online.

Το μόνο που πρέπει να κάνει ο "κακός" είναι απλά να ανακτήσει μια πραγματική σελίδα από το Web, πρωτού δημιουργήσει ένα αντίγραφο αυτής της σελίδας στο "ψεύτικο" Web.

Το κλειδί στην όλη υπόθεση είναι η τοποθέτηση του Web server του κακού, μεταξύ του "θύματος" και του υπόλοιπου Web. Η πρώτη κίνηση του "κακού" είναι να "ξαναγράψει" όλες τις URL διευθύνσεις σε μια Web σελίδα, ώστε να "δείχνουν" στον server του, αντί για έναν πραγματικό server. Ας υποθέσουμε ότι ο server του "κακού" είναι στη διεύθυνση www.attacker.org. Ο "κακός" ξαναγράφει ένα URL προσθέτοντας το http://www.attacker.org μπροστά από αυτό το URL. Για παράδειγμα,η διεύθυνση http://home.netscape.com γίνεται http://www.attacker.org/http://home.netscape.com

Το σχήμα δείχνει τί συμβαίνει όταν το "θύμα" κάνει αίτηση για μια σελίδα επιλέγοντας μια εκ των "ξαναγραμμένων" URL διευθύνσεων. Ο browser του "θύματος" ζητάει την προσπέλαση της σελίδας από τον www.attacker.org, εφόσον η πραγματική URL διεύθυνση αρχίζει με http://www.attacker.org. Το υπόλοιπο κομμάτι της URL διεύθυνσης, λέει στον server του "κακού" πού να ψάξει στο Web ώστε να λάβει το πραγματικό document. Ο server του "κακού" ζητάει και αποκτά την πραγματική σελίδα. Αφ'ότου αποκτήσει το πραγματικό document, τροποποιεί όλες τις URL διευθύνσεις που υπάρχουν στο document αυτό, βάζοντας μπροστά από αυτές τις διευθύνσεις τη διεύθυνση http://www.attacker.org. Τέλος, στέλνει την τροποποιημένη πλέον σελίδα στον browser του χρήστη. Εφόσον όλα τα URLs που υπάρχουν στη σελίδα "δείχνουν" στο http://www.attacker.org, εαν το "θύμα" ακολουθήσει ένα οποιοδήποτε



Παράδειγμα συναλλαγής στο Web κατά τη διάρκεια μιας Web spoofing επίθεσης.

(1) Ο browser του "θύματος" ζητάει τη σελίδα από το server του "κακού"
(2) Ο server του "κακού" ζητάει τη σελίδα από τον πραγματικό server
(3) Ο πραγματικός sever προσφέρει τη σελίδα στο server του "δολιοφθορέα"
(4) Ο server του "κακού" ξαναγράφει τη σελίδα
(5) Ο server του "κακού" δίνει την καινούρια έκδοση της σελίδας στο "θύμα".

link στη σελίδα που λαμβάνει, τότε η σελίδα αυτή θα ανακτηθεί πάλι μέσω του "κακού"

server. Το θύμα έτσι παραμένει παγιδευμένο στο "ψεύτικο" Web, και ενδέχεται να ακολουθεί links εσαεί, χωρίς να το εγκαταλείπει.

Εαν το "θύμα" συμπληρώσει μια φόρμα, σε μια σελίδα στο υποτιθέμενο Web, το αποτέλεσμα φαίνεται ότι παραδίδεται κανονικά. Όπως εξομοιώνεται η URL διεύθυνση, έτσι εξομοιώνεται και μια οποιοδήποτε φόρμα. Αυτό συμβαίνει διότι οι φόρμες υλοποιούνται μέσω των βασικών Web πρωτοκόλλων: οι υποβολές φορμών κωδικοποιούνται σε URLs και οι απαντήσεις δίνονται με HTML. Επομένως, εφόσον μπορεί να εξομοιωθεί ένα URL, το ίδιο ισχύει και για μια φόρμα.

Όταν το "θύμα" υποβάλλει μια φόρμα, τα δεδομένα πηγαίνουν απευθείας στον server του "κακού". Ο "κακός" μπορεί να παρατηρήσει, ακόμα και να τροποποιήσει τα δεδομένα της φόρμας, πριν την περάσει στον πραγματικό server. Μπορεί επίσης να τροποποιήσει τα δεδομένα που επιστρέφονται από τον πραγματικό server, ως απάντηση στην υποβολή μιας φόρμας.

Όπως αναφέραμε και προηγουμένως, η επίθεση που γίνεται δεν μπορεί να ανιχνευτεί, ακόμα και αν ο χρήστης έχει μια ασφαλή σύνδεση (μέσω SSL) με έναν server. Ο browser του, δείχνει πως η σύνδεση είναι ασφαλής, διότι πράγματι είναι ασφαλής. Ο browser δηλαδή του θύματος νομίζει πως όλα είναι μια χαρά: του είπαν να συνδεθεί στον www.attacker.org, και αυτός έκανε μία ασφαλή σύνδεση με τον www.attacker.org. Το εικονίδιο ασφαλής σύνδεσης στο περιβάλλον του browser, δίνει στο χρήστη μια ψευδαίσθηση ασφαλής σύνδεσης.

Αυτό που δεν αναφέραμε εως τώρα, είναι το πώς ο "κακός" πείθει τον χρήστη να εισέλθει στο ψεύτικο Web. Υπάρχουν αρκετοί τρόποι να συμβεί αυτό. Για παράδειγμα, εαν το "θύμα" χρησημοποιεί έναν Web-enabled E-mail client, ο "κακός" μπορεί να του στείλει E-mail, το οποίο θα περιέχει ένα link στο ψευτο-Web. Υπάρχουν άραγε τρόποι ανίχνευσης, από την πλευρά του χρήστη, της επίθεσης η οποία του γίνεται; σίγουρα υπάρχουν, αλλά ορισμένοι από αυτούς αντιμετωπίζονται από έναν ικανό δολιοφθορέα:

- **Η status line (γραμμή κατάστασης):** Η status line είναι μια απλή γραμμή κειμένου στο κάτω τμήμα του browser παραθύρου, η οποία επιδεικνύει διάφορα μηνύματα, κυρίως σχετικά με την πορεία της μεταφοράς δεδομένων μέσω του Web. Η επίθεση που περιγράφτηκε νωρίτερα, αφήνει δύο ίχνη στην Status line. Πρώτον, όταν το ποντίκι (mouse) βρίσκεται επάνω από ένα Web link, η status line επιδεικνύει το URL στο οποίο δείχνει ο σύνδεσμος. Έτσι, το "θύμα" ενδέχεται να προσέξει ότι ένα URL έχει τροποποιηθεί. Δεύτερον, όταν ανακτάται μια σελίδα, η Status line δείχνει το όνομα του server με τον οποίο γίνεται η σύνδεση. Έτσι, το θύμα μπορεί να παρατηρήσει το όνομα www.attacker.org. να εμφανίζεται στην Status line.
- **Η Location line (γραμμή τοποθεσίας):** Η Location line του browser επιδεικνύει το URL της σελίδας που προσπελαύνεται την τρέχουσα στιγμή. Το θύμα επίσης μπορεί να πληκτρολογήσει ένα URL στη Location line, στέλνοντας τον browser σε αυτή τη διεύθυνση. Η επίθεση που περιγράφτηκε προηγουμένως, δείχνει το τροποποιημένο URL στη Location line, δίνοντας στο χρήστη τη συνατότητα να ανακαλύψει την επίθεση. Αυτό το ίχνος μπορεί να παρακαμφθεί χάρη στα JavaScript προγράμματα. Ένα javascript πρόγραμμα μπορεί να κρύψει την πραγματική διεύθυνση και να την αντικαταστήσει με τη ψεύτικη διεύθυνση, η οποία φαίνεται σωστή. Έτσι, η "ψεύτικη" Location line, δείχνει στο χρήστη τη διεύθυνση που περιμένει να δει. Επίσης, η "ψεύτικη" Location line,δέχεται δεδομένα εισόδου από το πληκτρολόγιο, επιτρέποντας στο χρήστη να

πληκτρολογήσει ένα URL φυσιολογικά. Στη συνέχεια, το URL μπορεί να τροποποιηθεί από το javascript πρόγραμμα, προτού επιχειρηθεί η πρόσβαση του browser.

- **Ο πηγαίος κώδικας του document:** Υπάρχει ένα στοιχείο, το οποίο ο δολιοφθορέας δε μπορεί να παρακάμψει, αλλά και που είναι επίσης δύσκολο να παρατηρηθεί από το χρήστη. Χρησιμοποιώντας την επιλογή του browser 'view source' ('δες τον πηγαίο κώδικα'), το "θύμα" μπορεί να δει τον HTML κώδικα για τη σελίδα στην οποία βρίσκεται. Βλέποντας τις τροποποιημένες URL διευθύνσεις στον HTML κώδικα, το "θύμα" μπορεί να ανακαλύψει την επίθεση. Συνήθως όμως, οι περισσότεροι χρήστες και ιδίως οι αρχάριοι δεν ενδιαφέρονται για τον HTML κώδικα μιας σελίδας, οπότε και είναι περισσότερο ευάλωτοι σε τέτοιου είδους επιθέσεις. Μία άλλη επιλογή που μπορεί να αποβεί χρήσιμη, είναι η **'view document information'** ('δες πληροφορίες για το document') που υπάρχει σε ένα από τα μενού στο περιβάλλον του browser. Αυτή η επιλογή δείχνει πληροφορίες για το document συμπεριλαμβανομένης και της πραγματικής διεύθυνσης του document, δίνοντας έτσι ευκαιρία στο "θύμα" να συνηδειτοποιήσει την άσχημη κατάσταση στην οποία έχει περιέλθει.
- **Bookmarks:** Ο χρήστης επιλέγοντας ένα bookmark, υπάρχει περίπτωση να ξεφύγει από το ψευτο-Web, ή ακόμα μπορεί να έχει το ίδιο αποτέλεσμα επιλέγοντας την **'open location'** ('άνοιξε διεύθυνση') επιλογή από το μενου του browser, επιστρέφοντας έτσι στο πραγματικό Web. Βέβαια, το "θύμα"μπορεί να ξαναμπεί στο ψευτο-Web, επιλέγοντας το κουμπί 'back' ('πίσω'). Υπάρχει περίπτωση δηλαδή ο χρήστης να παλινδρόμεί ανάμεσα στο πραγματικό και το ψευτο-Web.

5.5.1.1 Μέτρα πρόληψης

Βραχυπρόθεσμα, η καλύτερη στρατηγική συνίσταται σε τρεις ενέργειες:

(1) Απενεργοποίηση του javascript στον browser, έτσι ώστε ο "κακός" να μην μπορεί να κρύψει τα ίχνη της επίθεσής του.
(2) Εξασφάλιση ότι η Location line είναι πάντα ορατή στο περιβάλλον του browser.
(3) Προσοχή στα μηνύματα της Location line του browser, έτσι ώστε να είναι σίγουρο ότι "δείχνουν" τον επιθυνητό server.

Την παρούσα στιγμή, οι javascript, ActiveX και Java τείνουν να διευκολύνουν το spoofing και άλλες επιθέσεις σε θέματα ασφαλείας, οπότε σε ορισμένες περιπτώσεις είναι ζωτικής σημασίας η απενεργοποίησή τους. Έτσι βέβαια υπάρχει μείωση της λειτουργικότητας του browser, αλλά στην καλύτερη περίπτωση θα πρέπει να επανενεργοποιούνται εφόσον υπάρχει σύνδεση με έναν "έμπιστο" server που απαιτεί την ύπαρξή τους.

Μακροπρόθεσμα, για σελίδες οι οποίες ανακτώνται μέσω μιας ασφαλούς σύνδεσης (π.χ SSL), θα πρέπει να υπάρχει ένα βελτιωμένο εικονείδιο στον browser, που θα προσδιορίζει όχι μόνο την ασφαλή σύνδεση, αλλά και το όνομα όποιου είναι στην άλλη πλευρά της σύνδεσης (το όνομα του server).

Φυσικά, τέλος, οι χρήστες θα πρέπει να είναι προσεκτικοί και να εκμεταλλεύονται όλες τις δυνατότητες που τους παρέχει ο browser τους, ώστε να μην πέφτουν εύκολα θύμα.

5.6 HTTP Cookies

Η πλήρης ονομασία των cookies είναι Persistent Client State HTTP Cookies . Ουσιαστικά, ένα cookie είναι δεδομένα που στέλνει ο server στον browser, όταν ο δεύτερος επισκέπτεται ένα Web site για πρώτη φορά. Τα δεδομένα αυτά ο browser τα αποθηκεύει καταρχήν στη μνήμη, και κατόπιν στο σκληρό δίσκο. Ο browser στη συνέχεια επιστρέφει αυτά τα δεδομένα στον server, ως τμήμα κάθε αίτησης προς τον server.

Όταν ένας Web server δέχεται μια αίτηση η οποία περιέχει ένα cookie (βρίσκεται στο HTTP header), υποτίθεται ότι τοποθετεί τα περιεχόμενά του σε μια μεταβλητή περιβάλοντος ("HTTP_COOKIE") πριν εκτελέσει οποιοδήποτε CGI πρόγραμμα, ως αποτέλεσμα της αίτησης. Έτσι, κάθε CGI πρόγραμμα μπορεί να κάνει χρήση των δεδομένων που είναι αποθηκευμένα στο cookie.

Αποθηκεύοντας πληροφορίες σε βάση δεδομένων

Συνήθως, οι πληροφορίες που αποκτώνται από τα cookies καταχωρούνται σε μια βάση δεδομένων, για περαιτέρω επεξεργασία. Για το σκοπό αυτό, μπορούν να χρησιμοποιηθούν εργαλεία αποθήκευσης δεδομένων όπως mSQL, Oracle, Sybase. Το ερώτημα που τίθεται, είναι "ποιά πληροφορία θα χρησιμοποιηθεί ως κλειδί για την προσπέλαση της βάσης". Η απάντηση είναι απλή: αν υποθέσουμε ότι ο χρήστης συμπληρώνει δεδομένα σε μια HTML φόρμα, και ότι το CGI script που χειρίζεται το input του χρήστη βρίσκεται σε μια περιοχή του server που απαιτεί οι χρήστες να συνδέονται (log-in) μέσω βασικής αυθεντικοποίησης, τότε μπορεί να χρησιμοποιηθεί η μεταβλητή περιβάλλοντος REMOTE_USER.

Συνδυάζοντας τα cookies με τη βάση δεδομένων

Στο προηγούμενο παράδειγμα, αποθηκεύσαμε πληροφορίες για τον χρήστη σε μια βάση δεδομένων στον Web server, τις οποίες πληροφορίες μπορούμε να ανακτήσουμε όποτε επιθυμούμε. Ένα προφανές χρονικό σημείο που θα επιθυμούσαμε να ανακτήσουμε την πληροφορία αυτή, θα ήταν η στιγμή που ο χρήστης επιστρέφει στο site. Σε αυτήν τη στιγμή, θα θέλαμε να γνωρίζουμε ότι ο συγκεκριμένος χρήστης έχει επισκεφτεί το site στο παρελθόν. Εαν αυτό ισχύει, συγκεντρώνουμε πληροφορίες για το χρήστη και τις χρησιμοποιούμε για να αλλάξουμε την HTML σελίδα που του στέλνουμε. Εαν ο χρήστης έχει δεχθεί ένα cookie που περιέχει το USER ID του, τότε μπορούμε να χρησιμοποιήσουμε την πληροφορία αυτή στο cookie ως κλειδί για την προσπέλαση της εγγραφής του χρήστη στη βάση δεδομένων. Στο προηγούμενο παράδειγμα, ο server απέκτησε το όνομα του χρήστη χάρη στη βασική αυθεντικοποίηση.

.

Μέθοδοι ανάλυσης δραστηριότητας

Τα cookies από μόνα τους δεν συνιστούν επαρκή ανάλυση της δραστηριότητας των χρηστών, αφού τα cookies καθ'αυτά δεν αποθηκεύουν οποιαδήποτε πληροφορία στον Web server. Επομένως, ακόμα και αν κάθε χρήστης που επισκέπτεται το site έχει ένα μοναδικό cookie, δεν παρατηρείται αλλαγή στα log αρχεία, εκτός και αν ο server κάνει κάτι με τις πληροφορίες που υπάρχουν στο cookie.

Η χρήση αποκλειστικά και μόνο των standard log αρχείων από την άλλη, δεν βοηθάει πολύ, καθώς οι standard log είσοδοι δεν καθορίζουν σε ποιόν χρήστη αντιστοιχεί η κάθε είσοδος. Επιπρόσθετα, το όνομα domain ή η IP διεύθυνση δεν είναι πάντα χρήσιμη πληροφορία, καθώς οι χρήστες που συνδέονται μέσω proxy servers εμφανίζουν την ίδια IP διεύθυνση, ενώ δεν είναι λίγοι οι χρήστες που έχουν δυναμικές (dynamically assigned) IP διευθύνσεις, οι οποίες συνήθως αλλάζουν κάθε φορά

που ο χρήστης επισκέπτεται το site. Όμως, εαν κάθε χρήστης που επισκέπτεται το site έχει ένα cookie που περιέχει ένα μοναδικό κωδικό, τότε μπορεί να αναλυθεί αποτελεσματικά η δραστηριότητα του κάθε χρήστη.

5.6.1 Ασφάλεια και cookies

Σήμερα τα cookies δημιουργούν αρκετές τριβές στην κοινότητα των χρηστών του Web . Υπάρχουν ορισμένοι που πιστεύουν ότι τίθετα θέμα εμπιστευτικότητας των πληροφοριών και ιδιωτικής ζωής των χρηστών, που δέχονται σε μεγάλη ποσότητα και συνήθως χωρίς καμία προειδοποίηση cookies από Web servers. Η αλήθεια είναι πως, παρότι τα cookies υποστηρίζονται από τον Internet Explorer από τις αρχές του 1996, η ύπαρξή τους έμεινε μυστική για αρκετά μεγάλο χρονικό διάστημα από τους χρήστες, κάτι που προκάλεσε πολλά ερωτηματικά. Η μόνη ένδειξη ύπαρξής τους, είναι ένα αρχείο που καλείται 'cookies.txt', το οποίο θα εντοπίσουν στο σκληρό τους όλοι οι χρήστες των δυο δημοφιλών browsers.

Συχνά, ορισμένα sites αποθηκεύουν στο cookies.txt του χρήστη εμπιστευτικές πληροφορίες όπως το password του χρήστη ή κωδικούς πιστωτικών καρτών. Με τις τεχνολογίες που υπάρχουν σήμερα στο Web, ο σκληρός δίσκος του χρήστη δεν είναι πλέον ασφαλής, πόσο μάλλον το αρχείο cookies.txt, το οποίο βρίσκεται πάντα σε συγκεκριμένο κατάλογο στο δίσκο. Επομένως, τα sites που αποθηκεύουν σημαντικές πληροφορίες, θα έπρεπε να προειδοποιούν το χρήστη, ώστε να προστατεύσει το αρχείο από μη εξουσιοδοτημένη πρόσβαση.

Πολλοί υποστηρίζουν πως δεν έχει αποσαφηνιστεί αρκετά ο τρόπος λειτουργίας των cookies, και οι δυνατότητες που έχουν . Σίγουρα, το γεγονός ότι οι Web servers απέκτησαν το δικαίωμα να "γράφουν" στο σκληρό δίσκο των ανυποψίαστων χρηστών, προβληματίζει αρκετούς. Αν μάλιστα λάβουμε υπ'όψιν μας και το γεγονός ότι χιλιάδες διαφημιστικά e-mails στέλνονται καθημερινά σε χρήστες, με βάση πληροφορίες που αναγράφονται στα cookies, τότε ο προβληματισμός αυτός γίνεται μεγαλύτερος.

5.7 Ιοί και Internet

Το Internet είναι ένα λειτουργικό μέσο. Μπορούμε να βρούμε οποιαδήποτε πληροφορία και να επικοινωνήσουμε με οποιονδήποτε χρήστη, ανταλλάσσοντας μηνύματα και αρχεία. Το πρόβλημα είναι ότι σε πολλές περιπτώσεις το αρχείο που βρήκαμε μετά από πολύ καιρό αναζήτησης, μπορεί να παρέχει και μερικές εντελώς ανεπιθύμητες παρενέργειες που ο κατασκευαστής δεν είχε την πρόθεση να περιλάβει στο πρόγραμμα. Στη διάρκεια όμως της διανομής αυτού του προγράμματος, έχει ενσωματωθεί και κάποιος ιός, που με την εγκατάσταση της εφαρμογής στον υπολογιστή μας θα ξεκινήσει τη λειτουργία του θέτοντας σε σημαντικό κίνδυνο την ακεραιότητα των πολύτιμων δεδομένων μας.

Οι ιοί που διακινούνται στο Internet φτάνουν τις μερικές χιλιάδες και λόγω της φύσης του μέσου, η διάδοσή τους είναι σε πολλές περιπτώσεις θέμα ωρών. Παλαιότερα, όταν οι δισκέτες αποτελούσαν το κύριο μέσο ανταλλαγής δεδομένων και shareware προγραμμάτων, για την προσβολή των υπολογιστών σε μία ευρεία γεωγραφική περιοχή ίσως θα έπρεπε να περάσουν και μήνες. Στο μεταξύ οι κατασκευαστές των antivirus προγραμμάτων διέθεταν το κατά περίπτωση κατάλληλο αντίδοτο και ελάχιστοι ήταν εκείνοι που αντιλαμβάνονταν την ύπαρξη του ίδιου του ιού. Η διάδοση του Internet όμως οφέλησε τους ιούς, όπως ακριβώς τα σύγχρονα συγκοινωνιακά μέσα οφέλησαν τη μετάδοση του ιού της γρίππης. Ενώ παλαιότερα θα έπρεπε να περάσει αρκετός χρόνος για να "ταξιδέψει" ένας ιός από τις ΗΠΑ στην Ευρώπη, σήμερα κάτι τέτοιο χρειάζεται μερικές μόνο ώρες. Οποιοσδήποτε μπορεί να συνδεθεί με κάποιο απομακρυσμένο ftp site για να αποκτήσει ένα

πρόγραμμα. Αν αυτό περιλαμβάνει και κάποιο ιό, ο αριθμός των υπολογιστών που μπορούν να προσβληθούν αυξάνεται εκθετικά. Οι κυριότερες κατηγορίες Ιών που θα συναντήσουμε στο Internet είναι οι εξής:

α) Γνωστοί και κλασικοί Ιοί: Αυτή η ομάδα των ιών θα μπορούσε να χαρακτηριστεί ως η κλασική. Περιλαμβάνει όλους τους ιούς που γνωρίζουμε εδώ και αρκετά χρόνια και απειλούν την ακεραιότητα των συστημάτων μας διαρκώς. Για τη συντριπτική πλειοψηφία των συγκεκριμένων ιών υπάρχουν δημοφιλή antivirus προγράμματα και σε γενικές γραμμές τα προβλήματα που μπορούν να προκαλέσουν στον χρήστη είναι ελάχιστα. Ακόμη και στην περίπτωση που πρόκειται για εντελώς νέες παρουσίες, οι μέθοδοι αντιμετώπισης είναι γνωστές αφού βασίζονται σε παλαιότερους ιούς. Οι πιο δύσκολοι στην αντιμετώπιση είναι οι ιοί που προσβάλουν τον boot sector του συστήματος και οι ιοί που επηρεάζουν το partition table του σκληρού δίσκου.

β) Ιοί Μακροεντολών: Οι ιοί που ανήκουν σ' αυτή την κατηγορία δεν αποτελούν εκτελέσιμα τμήματα κώδικα, αλλά εκμεταλλεύονται το μηχανισμό μακροεντολών που περιλαμβάνουν δημοφιλείς εφαρμογές. Οι διασημότεροι ιοί της συγκεκριμένης κατηγορίας είναι αυτοί που επηρρεάζουν το περιβάλλον εργασίας του Word.

Στην ουσία πρόκειται για μακροεντολές που αντιμετωπίζονται σχετικά εύκολα, όμως δεν υπάρχουν μέχρι στιγμής αυτόματες μέθοδοι ανίχνευσής τους πράγμα που διευκολύνει σημαντικά τη διάδοσή τους. Κάποια στιγμή ακόμη και στις κεντρικές εγκαταστάσεις της Microsoft αναφέρθηκαν κρούσματα προσβολής από τους συγκεκριμένους ιούς. Πάρα πολλοί χρήστες ανταλλάσουν μέσω του ηλεκτρονικού ταχυδρομείου, έγγραφα τα οποία έχουν δημιουργηθεί στο Word και για το λόγο αυτό ο ρυθμός διάδοσης των συγκεκριμένων ιών είναι εξαιρετικά υψηλός.

γ) Ιοί Java και JavaScript: Αυτή η ομάδα ιών είναι ίσως και η πιο επικίνδυνη. Οι ειδικοί πιστεύουν ότι πάρα πολύ σύντομα θα κληθούμε να αντιμετωπίσουμε τους ιούς που έχουν κατασκευαστεί με τη γλώσσα Java ή την JavaScript.

Το γεγονός ότι οι συγκεκριμένες γλώσσες αποδεικνύονται εξαιρετικά ισχυρές, έχει δημιουργήσει αρκετές ανησυχίες, αφού κάποιος με αρκετές γνώσεις στην Java θα μπορούσε να δημιουργήσει ένα applet, το οποίο θα τρέχει στον Web browser του ανυποψίαστου χρήστη, προκαλώντας άπειρα προβλήματα. Η κύρια μέθοδος αντιμετώπισης είναι η απενεργοποίηση της επιλογής για την εκτέλεση των applets που έχουν γραφτεί σε Java ή JavaScript.

δ) Trojan Horses ή Δούρειοι Ίπποι: Στην περίπτωση αυτή έχουμε ένα τμήμα ανεπιθύμητου κώδικα κρυμμένου μέσα σε ένα τμήμα επιθυμητού κώδικα. Προμηθευόμαστε, δηλαδή, ένα πρόγραμμα το οποίο εκτελεί ή υποστηρίζει ότι εκτελεί μια επιθυμητή λειτουργία και μόλις το χρησιμοποιήσουμε (είτε αμέσως είτε μόλις ικανοποιηθεί μια λογική ή χρονική συνθήκη), αυτό κάνει και κάτι άλλο, συνήθως ανθυγιεινό για τον υπολογιστή. Υπάρχει μία μικρή ομάδα ιών που ανήκουν στην κατηγορία των Δούρειων Ίππων και που αφορούν πρωτίστως τους χρήστες του Intenet, καθώς και όσους χρησιμοποιούν Shareware προγράμματα. Πρόκειται για ιούς που εμφανίζονται με το όνομα κάποιου γνωστού προγράμματος.Αν επιχειρήσουμε να τρέξουμε το πρόγραμμα ο ιός ξεκινά άμεσα τη λειτουργία του και συνήθως διαγράφει τα αρχεία του σκληρού δίσκου.

ε) Ιοί Ηλεκτρονικού Ταχυδρομείου: Σε τακτά χρονικά διαστήματα εμφανίζονται διάφορα μηνύματα που προειδοποιούν τους χρήστες του Internet για την ύπαρξη μερικών "πονηρών" μηνυμάτων ηλεκτρονικού ταχυδρομείου, τα οποία μπορούν ακόμη και να "κάψουν" τον επεξεργαστή. Πιο διάσημος ιός εδώ είναι ο Good Times και πολλοί (νέοι κυρίως) χρήστες αναφέρονται σ' αυτόν με δέος. Υποτίθεται πως αν λάβουμε ένα μήνυμα με τον τίτλο Good Times και επιχειρήσουμε να το διαβάσουμε, αυτόματα θα διαγραφούν όλα τα αρχεία από το σκληρό δίσκο και μπορεί να υποστεί ανεπανόρθωτη βλάβη ακόμη και ο επεξεργαστής.

Φυσικά δεν υπάρχει μήνυμα ηλεκτρονικού ταχυδρομείου που μπορεί να εκτελέσει τέτοιου είδους λειτουργία. Για να λειτουργήσουν οι ιοί θα πρέπει κάποιος να τους ενεργοποιήσει, δηλαδή να εκτελέσει το πρόγραμμα που έχει προσβληθεί. Οι τύποι των ιών που κυκλοφορούν στο Internet και που μπορούν να προσβάλουν τον υπολογιστή μας είναι αρκετοί. Για κάθε μία ομάδα υπάρχουν κάποιες τεχνικές προστασίας και εξουδετέρωσης. Σε όλες τις περιπτώσεις εκείνο που απαιτείται από την πλευρά του χρήστη είναι να δράσει γρήγορα, για να περιορίσει τις τυχόν βλάβες που μπορούν να δημιουργηθούν. Να σημειώσουμε επίσης ότι υπάρχουν και κάποιοι ιοί που μοιάζουν με... φαντάσματα. Πολλοί χρήστες αναφέρονται σ' αυτούς αλλά κανείς δεν τους έχει δει να λειτουργούν στην πράξη. Στην πραγματικότητα πρόκειται για διαδόσεις, οι οποίες όμως πολλές φορές προκαλούν πανικό στους ανυποψίαστους χρήστες.

Αν ο χρήστης συμμετέχει σε κάποιο newsgroup ή σε μία δημοφιλή mailing list, η ενημέρωσή του για τους πιο επικίνδυνους ιούς είναι άμεση. Ανεξάρτητα από το θέμα που συζητιέται, κάποιος θα τον ενημερώσει για την ύπαρξη ενός νέου ιού. Υπάρχουν newsgroups και mailing lists όπου συζητούνται αποκλειστικά θέματα που έχουν να κάνουν με τη δημιουργία και την αντιμετώπιση των ιών. Οι διευθύνσεις των μεγαλύτερων εταιρειών κατασκευής antivirus προγραμμάτων , διαθέτουν εκτενείς καταλόγους και αναλυτικές πληροφορίες για τους ιούς και οι περισσότεροι διανέμουν public-domain προϊόντα που θωρακίζουν σε μεγάλο βαθμό το σύστημά.

Βιβλιογραφία

1. ANDREW S, TANENBAUM, "*Δίκτυα Υπολογιστών*", Εκδόσεις Κλειδάριθμος, Αθήνα 2003

2. JOE CASAD, "*Μάθετε το TCP/IP σε 24 ώρες*", Εκδόσεις Μ. Γκιούρδας, Αθήνα 2004

3. "*TCP Flooding and IP Spoofing*", CIAC Information Bulletin, http://ciac.llnl.gov/ciac/bulletins/g-48.shtml.

4. ΑΝΔΡΕΑΣ ΠΟΜΠΟΡΤΣΗΣ, "*Εισαγωγή στις νέες τεχνολογίες επικοινωνιών*" , Εκδόσεις Α. Τζιόλα Ε. , Θεσσαλονίκη 1997

5. FARMER DAN, "*Improving the Security of Your Site by Breaking Into it*", http://www.trouble.org/satan/admin-guide-to-cracking.html.

6. "*Checking your network security using TCP_WRAPPERS and SATAN*", NTUA Seminars, System Security: http://www.ntua.gr/seminars/sec/

7. ΆΡΗΣ ΑΛΕΞΟΠΟΥΛΟΣ και ΓΙΩΡΓΟΣ ΛΑΓΟΓΙΑΝΝΗΣ, "*Τηλεπικοινωνίες και Δίκτυα υπολογιστών*", Εκτη έκδοση, Αθήνα 2003

8. ΑΝΔΡΕΑΣ ΠΟΜΠΟΡΤΣΗΣ και ΓΕΩΡΓΙΟΣ ΠΑΠΑΔΗΜΗΤΡΙΟΥ, "*Ασφάλεια Δικτύων Υπολογιστών*", Εκδόσεις Τζιόλας, Θεσσαλονίκη 2003

9. ΓΕΩΡΓΙΟΣ ΠΑΓΚΑΛΟΣ και ΙΩΑΝΝΗΣ ΜΑΥΡΙΔΗΣ "*Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων*", Εκδόσεις ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη 2002

10. LINCOLN D. STEIN και JOHN N. STEWART , Φεβρουάριος 4, 2002 , http://www.w3.org/Security/Faq/

11. FREDERIC RAYNAL, "*Malicious cryptography*" , 8 Μαϊου 2006 , http://www.securityfocus.com/infocus/1865

12. PHIL KONSTENBADER και BOB DONELLY, "*Standards in desktop firewall Policies*" 6 Ιουνίου 2006, http://www.securityfocus.com/infocus/1867

13. RALF SENDEREK , "The protection of your Secret Key" , Οκτώβριος 2003 , http://senderek.de/security/secret-key.protection.html

14. PAUL GILSTER, "*Το Καλύτερο Βιβλίο για το Internet*" ,Εκδόσεις Μ.Γκιούρδας, Αθήνα 2003

15. ΣΩΚΡΑΤΗΣ ΚΑΤΣΙΚΑΣ , "*Προστασία και Ασφάλεια Συστημάτων Υπολογιστών*", Εκδόσεις Ελληνικό Ανοικτό Πανεπιστήμιο , Πάτρα 2001

16. DORI SMITH , "*Java 2 για τον παγκόσμιο ιστό*" , Εκδόσεις Κλειδάριθμος , Αθήνα 2003

17. PRINCET ON SECURE INTERNET PROGRAMMING TEAM , "*Java vs ActiveX*" , 28 Απριλίου 1997 , http://www.cs.princeton.edu/sip/faq/java-vs-activex.html

18. JEREMY CARL , "*ActiveX Security*" , 4 Νοεμβρίου 1996 , http://www.webdeveloper.com/activex/activex_security.html

19. ActiveX Tutorial , http://www.techiwarehouse.com/cms/engine.php?page_id=ab5ce018

20. Introduction to TCP/IP , http://www.w3schools.com/tcpip/tcpip_intro.asp

21. ELLIOTTE RUSTY HAROLD , "*Processing XML with Java*" , 2001,2002 , http://ftp.ibiblio.org/xml/books/xmljava/

22. How Kerberos Works , http://docs.hp.com/en/T1417-90001/ch01s04.html

23. "*Securing Internet Information Servers*" , CIAC team , Δεκέμβριος 1994 , http://www.ciac.org/ciac/documents/ciac2308.html

24. "*Virtual Private Network*" , http://www.iec.org/online/tutorials/vpn/topic01.html

25. Κ. Μάγκος και Α. Νιξαρλίδης , "*Ασφάλεια στο Διαδίκτυο*" , Ιούλιος 1999 , http://www.lab.epmhs.gr/gr/html/ptixiakes/kostasaris_ptyxiakh/Phtml/index.htm

26. "Internet Privacy and Confidentiality" , http://www.livinginternet.com/i/is_conf.htm

27. AVOLIO and BLASK , "Application Gateways and Stateful Inspection" , 22 Ιανουαρίου 1998 , http://www.avolio.com/papers/apgw+spf.html

28. "*Firewalls*" , http://www.securitytechnet.com/security/firewall.html

29. TONY BRADLEY , "Internet/Network Security" , 24 Ιουλίου 2006 , http://netsecurity.about.com/

30. MATT WELSH , "*Ο Οδηγός του Linux*" , Εκδόσεις Κλειδάριθμος , Αθήνα 2003.

31. "*Η Ασφάλεια στο Διαδίκτυο*" , http://00357.com/com/index/about-internet/data/astinomia/asfaleia.asp

32. "*Cryptography in the Real World:5.1 Security on the Internet*" , http://www.rsasecurity.com/rsalabs/node.asp?id=2153