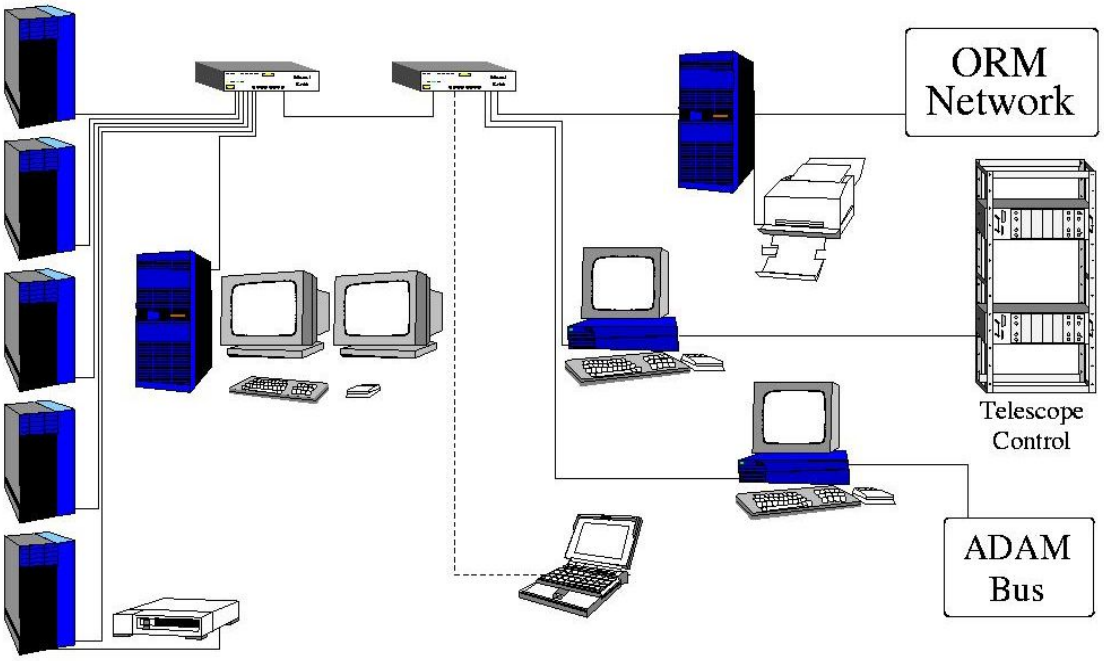
Τ.Ε.Ι ΗΠΕΙΡΟΥ
T.E.I OF EPIRUS

Σχολή Διοίκησης & Οικονομίας (Σ.Δ.Ο)
Τμήμα Τηλεπληροφορικής & Διοίκησης

School Of Management And Economics
Department Of Communications, Informatics And Management

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: ΑΣΦΑΛΕΙΑ ΣΤΟ TCP/IP ΚΑΙ ΣΤΟ WEB



ΑΛΕΞΑΝΔΡΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ Α.Μ. 2057

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΤΣΙΑΝΤΗΣ ΛΕΩΝΙΔΑΣ

ΠΕΡΙΕΧΟΜΕΝΑ

Το World Wide Web αποτελεί τη μεγαλύτερη πηγή πληροφοριών σήμερα στον κόσμο, καθώς πλησιάζουμε στον εικοστό πρώτο αιώνα. Το εντυπωσιακότερο ίσως στοιχείο είναι ότι εξελίσσεται με τέτοιον ιλιγγιώδη ρυθμό, ώστε να τρομάζει όσους προσπαθούν να κατανοήσουν τις τεχνολογίες που το διέπουν. Μεταξύ αυτών συγκαταλέγομαι και εγώ…

Το Internet, κάποτε ήταν προνόμιο των "Πατρικίων". 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.

Μια μέρα ρουτίνας αρχίζει: ξυπνάω, διαβάζω την εφημερίδα μου, ενημερώνομαι για τις μετοχές μου στο χρηματιστήριο, λέω μια βιαστική καλημέρα στο φίλο μου το Γιώργο που φαίνεται κάπως αγουροξυπνημένος (μάλλον νυσταγμένος θα είναι, αφού στην Αμερική τώρα είναι βράδυ), περνάω μια βόλτα από τη βιβλιοθήκη στο πανεπιστήμιο του Essex να δω αν επιτέλους ήλθε το βιβλίο που ψάχνω τόσο καιρό, κλείνω ραντεβού με τον οδοντίατρό μου για το απόγευμα, βάζω ROCK-FM, βλέπω την αγαπημένη μου εκπομπή στο CNN, πετάγομαι και αγοράζω τις μπότες που είχα σταμπάρει από χθες το βράδυ και… επιτέλους σηκώνομαι από τον υπολογιστή μου (έχω ψηφιακό τηλέφωνο, αρκετές μονάδες έπεσαν).

Ίσως φαντάζει, αλλά δεν είναι πολύ μακρινή αυτή η εικόνα. Σε λίγο καιρό, το Web θα έχει γίνει χώρος πλήρωσης κάθε δραστηριότητας. Το αν αυτό είναι αρνητικό ή θετικό, επιδέχεται συζητήσεων.

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, ανταλλάσονται 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. Ελπίζω πως από τη μελέτη αυτή μπορεί να βοηθηθεί τόσο ο υπεύθυνος δικτύου, όσο και ο απλός χρήστης. Όσο καιρό ασχολήθηκα με αυτήν την εργασία,

βρέθηκα αντιμέτωπος με καινούρια δεδομένα, που ανέτρεπαν αρκετά από αυτά που είχα διαβάσει έως εκείνη τη στιγμή. Προσπάθησα να είμαι όσο το δυνατόν περισσότερο κοντά στις εξελίξεις, κάτι που ως ένα βαθμό νομίζω πως το κατάφερα. Είμαι σίγουρος όμως, πως σε λίγους μήνες, ένα μεγάλο τμήμα των στοιχείων που παραθέτω, θα θεωρείται ξεπερασμένο. Αυτό είναι ίσως και το τίμημα της μελέτης μιας τόσο απρόβλεπτης δομής, όπως είναι το Web και οι μηχανισμοί ασφάλειας που φιλοδοξούν να το προστατεύσουν.

Για ένα μεγάλο χρονικό διάστημα, αναλώθηκα σε σκέψεις σχετικά με το ποιά θα

έπρεπε να είναι η δομή της εργασίας μου. Όποιο θέμα και αν εξέταζα, ήταν άρρηκτα συνδεδεμένο με κάποιο άλλο. Ξεκινώντας με γνωστικά πεδία που αφορούσαν αμιγώς το Web, συνηδειτοποίησα ότι δε θα μπορούσα να αγνοήσω σημαντικές παραμέτρους που σχετίζονταν με τα TCP/IP δίκτυα γενικότερα και τις υπηρεσίες που παρέχονται σε αυτά.
Έτσι, προσπαθώντας να ξετυλίξω το κουβάρι που λέγεται “ασφάλεια στο Web”, βρέθηκα αντιμέτωπος με θέματα που αφορούσαν την ασφάλεια στο Internet γενικότερα, και τα οποία δε μπορούσα να αμελήσω. Ως αποτέλεσμα, παρέκκλινα ελαφρώς από την αρχική μου κατεύθυνση, και συμπεριέλαβα στη μελέτη μου προβλήματα με τα οποία δε σκόπευα να ασχοληθώ εξαρχής. Ελπίζω να μην αποδειχθώ εκτός θέματος.
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.

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 **[80]**. Γι' αυτόν το λόγο, 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. Κατά βάση, σ' αυτό
υπάρχει μια μεγάλη δόση αλήθειας. 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 καλωσύνη. 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.

Ποιό πρωτόκολλο χρησιμοποιείται?

Η επίτευξη της λειτουργίας των υπολογιστών απαιτεί το σωστό πρωτόκολλο. Στην αργκό 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, γι’
αυτό και θα αποτελέσει σημείο αναφοράς μας στη συνέχεια του πονήματος.

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 ηλεκρονικού
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. Αυτή η διαδικασία
περιγράφεται από ένα υψηλής τεχνολογίας όρο -asynchronous communications (ασύγχρονες επικοινωνίες). Ο όρος σημαίνει ότι οι λειτουργίες κλήσης και απάντησης
δεν είναι απαραίτητο να συμβούν ταυτόχρονα σεμία τέτοιου είδους επικοινωνία. Οι διευθύνσεις e-mail των χρηστών στο Internet είναι της μορφής user@host.domain (π.χ η διεύθυνσης του γράφοντος είναι macman@compulink.gr. Για
το σύστημα διευθυνσιοδότησης και ονομασίας στο Internet θα μιλήσουμε σε λίγο. 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 υπολγιστή. 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 (δυαδικά ή
αρχεία κειμένου) 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.

Όταν ο χρήστης επιθυμεί την ανάκτηση συγκεκριμένων αρχείων και δεν ξέρει σε ποιόν απομακρυσμένο υπολογιστή να συνδεθεί μέσω FTP, χρησιμοποιεί το εργαλείο
ARCHIE (αρχειοθέτης). Αυτό το εργαλείο οδηγεί στον εντοπισμό του αρχείου που αναζητεί ο χρήστης, ανεξάρτητα από την εγκατάσταση FTP στην οποία αυτό βρίσκεται.

Δημοφιλής client για Windows αυτή τη στιγμή είναι το WS-FTP, σε 16bit και 32bit μορφή.

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 ποιές 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 (που έχουν την μορφή *#channel*), 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 (τουλάχιστον έμμεσα) μεταξύ τους και κάθε φορά που ο
χρήστηςέρχεται 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 (θα αναφερθούμε στη συνέχεια), 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 συνδεση με πολλούς IRC

servers, με πολλά διαφορετικά κανάλια, όπως και την πιό φιλική για το χρήστη πλοήγηση
στον χαώδη, μέχρι και πριν από μερικά χρόνια, κόσμο του IRC.
Το client που χρησιμοποιείται ευρέως στα Windows 95 αυτήν τη στιγμή είναι το mIRC 32, version 5.02, από τον Khaled Mardam-Bey, και παρέχει τις δυνατότητες στις
οποίες αναφερθήκαμε.

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 (Ο Ιστός) 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 είναιένα 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). Clients για πλοήγηση στο Web έχουν υπάρξει αρκετοί για διάφορα ήδη υπολογιστικών και λειτουργικών συστημάτων: WWYSIWYG (1990), NCSA Mosaic (1991), Hotjava κ.λ.π. 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 (αυτή τη στιγμή διατίθενται οι εκδόσεις 4.0 των δύο browsers), οι οποίοι εκτός από φυλλομετρητές στον Ιστό έχουν ενσωματωμένους clients για ανάγνωση email,
USENET news, αλλά και δημιουργία HTML σελίδων, Java applets , VRML editors, ACTIVE X τεχνολογία κ.α.

Άλλες υπηρεσίες.

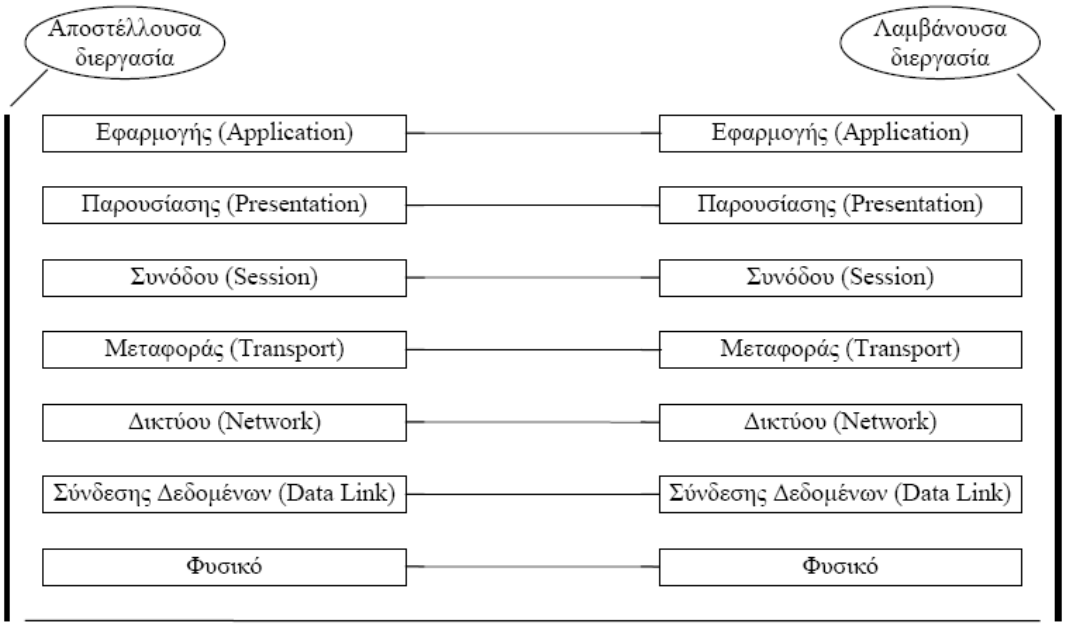
Άλλες υπηρεσίες στο Internet, όπως οι υπηρεσίες WAIS, Gopher, είναι υπηρεσίες αναζήτησης πόρων στο Internet, που όμως η "δημοτικότητά" τους εκφυλίστηκε με το
πέρασμα του χρόνου, εξ' αιτίας της ολοένα διαδεδομένης χρήσης του Web ως "μικροσκόπιο" του Διαδικτύου…

Ασφάλεια στο TCP/IP

1.1 Το μοντέλο OSI

Το 1983, ο Διεθνής Οργανισμός Τυποποίησης (ISO) πρότεινε το μοντέλο αναφοράς OSI (Open Systems Interconnection, Διασύνδεση Ανοιχτών Συστημάτων) **[1]**.
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 μεραφοράς, 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 **[2]**. 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 ανωτέρων 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, Σύνδσης Δεδομένων, Δικτύου).

		Παραδείγματα Πρωτοκόλλων
4	**Επίπεδο Εφαρμογής** συνίσταται σε εφαρμογές και διαδικασίες που χρησιμοποιούν το δίκτυο	HTTP
3	**Επίπεδο Μεταφοράς** παρέχει end-to-end υπηρεσίες διανομής δεδομένων	TCP
2	**Επίπεδο Internet** καθορίζει το datagram και χειρίζεται τη δρομολόγηση των δεδομένων	IP
1	**Επίπεδο Πρόσβασης Δικτύου** συνίσταται σε ρουτίνες για την πρόσβαση των φυσικών δικτύων	ARP

Σχήμα 2 Επίπεδα στην αρχιτεκτονική των TCP/IP πρωτοκόλλων

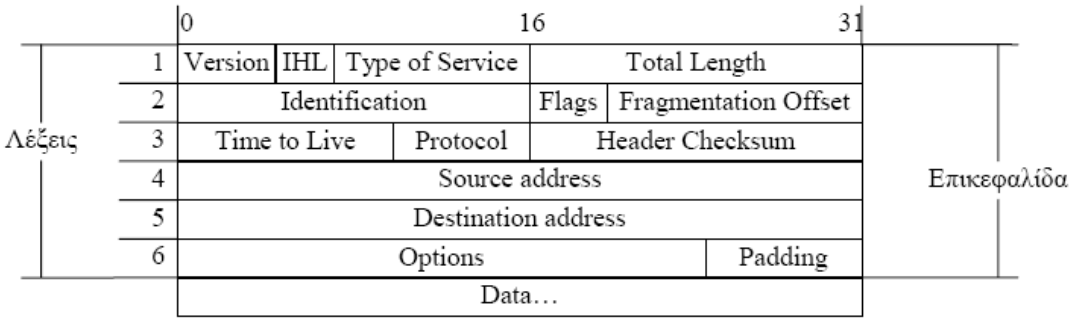
Οι λειτουργίες που επιτελούνται σε αυτό το επίπεδο περιλαμβάνουν ενθυλάκωση (πρόσθεση επικεφαλίδας) των IP datagrams στα frames** που μεταδίδονται από το δίκτυο, και η αντιστοίχιση των IP διευθύνσεων στις φυσικές διευθύνσεις που χρησιμοποιούνται από το δίκτυο.

Επίπεδο "Internet"

Το επίπεδο Internet είναι επάνω από το επίπεδο Πρόσβασης Δικτύου στην

ιεραρχία των πρωτοκόλλων. Το **Internet Protocol**, RFC 791, 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 (το λεγόμενο "handshake",που θα δούμε αργότερα) 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. Εαν 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 σωστο 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.

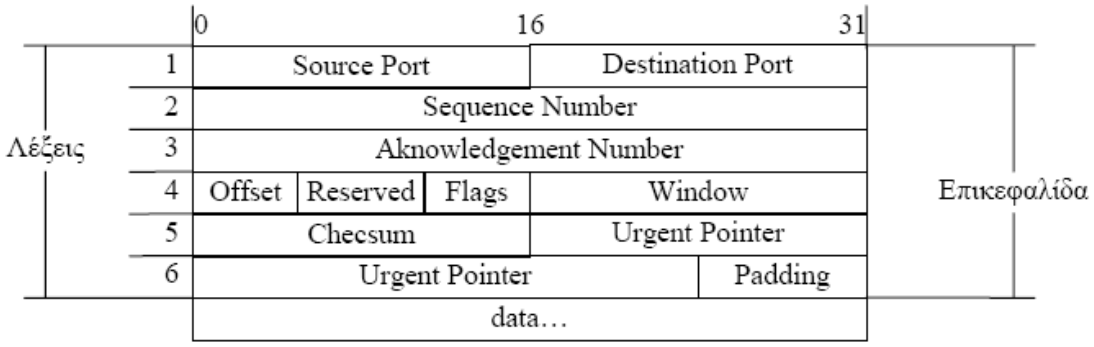


Σχήμα 3 Το format του IP datagram

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 ανταλλάσεται 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. Εαν τα δεδομένα έχουν παραβιαστεί, ο παραλήπτης τα *απαλάσσει* (discard). Μετά από μια λογική περίοδο διαλλείματος (timeout), ο αποστολέας ξανα-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), ανταλλάσονται 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.

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.
Κάθε byte δεδομένων αριθμείται σειριακά, με βάση το ISN, οπότε το πρώτο πραγματικό byte δεδομένων που στέλνεται έχει *αριθμό ακολουθίας* ISN+1 (συνήθως 1).
Το πεδίο "Sequence Number" στην επικεφαλίδα κάθε segment δεδομένων προσδιορίζει
τη "θέση", του πρώτου byte δεδομένων του segment, στη ροή των δεδομένων (data
stream). Για παράδειγμα, εαν το πρώτο byte στη ροή των δεδομένων έχει sequence number = 1 (ISN = 0) και έχουν ήδη μεταφερθεί 4000 bytes δεδομένων, τότε το πρώτο
byte στο τρέχων segment θα είναι το byte 4001, και το sequence number θα είναι ίσο με
4001.
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, εαν 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 ποιά 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 ποιά 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) εως 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 (RFC 826 και RFC 903).

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
[3]. Εξ'αιτίας μιας σειράς επιθέσεων αυτού του τύπου το 1996, αρκετοί ISPs (Παροχείς
Υπηρεσιών Internet) εξαφανίστηκαν από το δίκτυο.
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 ένας περιορισμένος αριθμός
εξελισσόμενων συνδέσεων επιτρέπεται, και αυτός ο αριθμός είναι συνήθως μικρότερος
του δέκα.
Ας συγκεκριμενοποιήσουμε την επίθεση, χρησιμοποιώντας την ορολογία του
TCP πρωτοκόλλου [4]. 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.
Ο επιτιθέμενος host στέλνει SYN αιτήσεις στην TCP port που επιθυμεί να απενεργοποιήσει. Πρέπει να σιγουρευτεί ότι η IP διεύθυνση πηγής είναι αλλαγμένη
(spoofing, βλέπε 1.3.2) ώστε να ισούται με τη διεύθυνση κάποιου άλλου, προς το παρόν
απροσέγγιστου host. Η IP διεύθυνση πρέπει να μη μπορεί να προσεγγιστεί, επειδή ο
επιτιθέμενος δεν επιθυμεί κάποιος host να δέχεται τα SYN/ACKs που θα προέρχονται
από τον host-στόχο (εαν συνέβαινε αυτό, θα είχε ως αποτέλεσμα την αποστολή στον
host-στόχο, ενός segment με το RST flag αληθές*** . Συμβολίζοντας ως Z(x) τον host Z
που προσποιείται ότι είναι ο x, και ως B τον host-στόχο, έχουμε:
1 Z(x) ---SYN B
* ftp://info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding
** socket είναι το μοναδικό ζεύγος (port - IP διεύθυνση) ενός client ή server.
*** Το RST flag (σημαία) είναι αληθές, όταν ο host που στέλνει το segment επιθυμεί το πέρας της
σύνδεσης. Στην περίπτωση μας αυτό είναι λογικό, καθώς ο host δέχεται πακέτα SYN/ACK χωρίς να έχει
στείλει προηγουμένως μια SYN αίτηση (την αίτηση την έστειλε ο επιτιθέμενος host).
Z(x) ---SYN B
Z(x) ---SYN B
Z(x) ---SYN B
Z(x) ---SYN B
… … …
2 x SYN/ACK --- B
x SYN/ACK --- B
x SYN/ACK --- B
… … …
3 x RST ------ B
Στο (1) ο επιτιθέμενος host Z στέλνει πολλαπλές SYN αιτήσεις προς τον host-
στόχο, ώστε να γεμίσει την backlog ουρά του με εκκρεμείς συνδέσεις. Στο (2) ο host-
στόχος απαντάει με SYN/ACKs σε αυτόν που νομίζει ότι έστειλε τα SYN πακέτα
(δηλαδή στον απροσέγγιστο host x). Εδώ πρέπει να τονίσουμε, ότι το IP μπορεί να

πληροφορήσει το TCP ότι ο host είναι απροσέγγιστος, αλλά το TCP θεωρεί αυτά τα λάθη προσωρινά και επαφίεται στο IP για την παράκαμψή τους (π.χ αναδρομολόγηση των πακέτων).

Κατ'αυτόν τον τρόπο, η δομή δεδομένων (ουρά) ή πίνακας που ο server χρησιμοποιεί ώστε να περιγράψει όλες τις εκκρεμείς συνδέσεις, υπερχειλίζεται [5], 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 επηρρεάζει τις ήδη υπάρχουσες εισερχόμενες συνδέσεις (για τις οποίες έχει γίνει τριπλό handshake), όπως επίσης δεν επηρρεάζει 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. Για παράδειγμα, στο SunOS, αυτό μπορεί να γίνει με την εντολή:

netstat -a -f inet

Εαν ένας μεγάλος αριθμός συνδέσεων, περιγράφεται με την κατάσταση "SYN_RECEIVED", τότε κάτι τέτοιο σημαίνει ότι το σύστημα δέχεται επίθεση.

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* (input source filtering), διαμορφώνοντας κατάλληλα τους δρομολογητές του δικτύου ή χρησιμοποιώντας firewalls. Έτσι, είναι απαραίτητοαφενός 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 [3], 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 (πάνω από
100 megabytes για ένα σύστημα με 25 εφαρμογές server).
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. Εαν 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 [6]. 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. Τα πρώτα 4 bytes της επικεφαλίδας είναι τα ίδια για κάθε ICMP μήνυμα, ενώ το υπόλοιπο της επικεφαλίδας διαφέρει για ICMP μηνύματα διαφορετικού είδους. Υπάρχουν 15 διαφορετικοί τύποι ICMP μηνυμάτων Οι τύποι οι οποίοι μας ενδιαφέρουν είναι ο τύπος 0x0 και ο 0x8. Ο ICMP τύπος 0x0 προσδιορίζει ένα ICMP_ECHOREPLY (η απάντηση) και ο 0x8 προσδιορίζει ένα ICMP_ECHO (η ερώτηση). Η κανονική ροή των γεγονότων είναι ένα ICMP_ECHO από τον client να προκαλεί ένα ICMP_ECHOREPLY από τον server (ο server είναι ουσιαστικά ο kernel του λειτουργικού συστήματος του host-στόχου).

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 (κάτι σαν timestamp), 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.

Παρ'ότι το payload είναι συνήθως πληροφορίες που αφορούν το χρόνο, δεν υπάρχει τρόπος να βεβαιωθεί αυτό. Έτσι, το περιεχόμενο του προαιρετικού αυτού
τμήματος δεδομένων μπορεί να είναι αυθάιρετο (arbitrary). Έτσι, trojan horses μπορούν
να ενθυλακωθούν σε ένα ICMP_ECHO πακέτο, με αρνητικά αποτελέσματα. Επιπλέον, ένας μεγάλος αριθμός ICMP_ECHO πακέτων είναι ικανός να
* Το τμήμα αυτό των δεδομένων αναφέρεται συχνά ως payload.
δημιουργήσει άρνηση υπηρεσίας σε έναν server** . Μάλιστα, το Νοέμβριο του 1996,
ανακαλύφθηκε ένα σοβαρό "λάθος" στις υλοποιήσεις των Windows 95 και NT της
Microsoft, η οποία ενσωμάτωσε την εντολή ping στα λειτουργικά της, χωρίς να
συμπεριλάβει τους απαραίτητους περιορισμούς για το μέγεθος του IP πακέτου* . Έτσι,
εαν κάποιος που είχε λειτουργικό Windows, έβγαινε στο prompt του DOS και έδινε την
εντολή:
ping -1 65510 host
θα έστελνε ένα πακέτο σε οποιονδήποτε υπολογιστή στο Internet. Μάλιστα, θα μπορούσε
να στείλει περισσότερα από ένα πακέτα, με την παράμετρο -n στην εντολή του. Δηλαδή:
ping -n 100 -1 65510 host
ώστε να αποστείλει εκατό πακέτα. Εαν ο χρήστης δει το μήνυμα "Request Timed Out",
τότε αυτό θα σημαίνει πως ο απομακρυσμένος host θα έχει καταρρεύσει.
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)
[7]. 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 [8]. Γενικά, η

** "Το Ping Του Θανάτου", ΚΟΣΜΟΣ ΤΟΥ INTERNET, σελ 94, Τεύχος 19, Ιανουάριος 1997.

* Τα IP πακέτα μπορούν να έχουν μέγεθος μέχρι 65.535 bytes, συμπεριλαμβανομένης της επικεφαλίδας
που είναι 20 bytes. Η ICMP_ECHO αποτελείται από 8 bytes επικεφαλίδας, ακολουθούμενα από τον αριθμό
που προσδιορίζουμε στη γραμμή των εντολών. Επομένως, το μέγιστο μέγεθος της επιτρεπόμενης data area
είναι 65.535-20-8=65.507 bytes

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 (ενότητα 1.3.1.1) 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 Α, 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 Α (τα οποία προορίζονται για τον έμπιστο host) δε φθάνουν ποτέ στο στόχο τους (αφού ο Β 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 Β δε μπορεί να απαντήσει.

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

Απαραίτητη προϋπόθεση για την επίθεση, είναι η γνώση ενός τουλάχιστον host που εμπιστεύεται ο host A. Εαν ο Α 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 Α".

Για να το κάνει αυτό, συνδέεται κανονικά (με _____την πραγματική του διεύθυνση) σε μια TCP port του Α (π.χ SMTP) και πραγματοποιεί μαζί του ένα τριπλό handshake, αποθηκεύοντας τον ISN (Initial sequence Number) που χρησιμοποίησε ο Α. 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 Α 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* (128,000/δευτερόλεπτο και 64,000 ανά σύνδεση), και γνωρίζει πόσος**
περίπου χρόνος θα χρειαστεί ώστε ένα IP datagram να ταξιδέψει στο Internet για να
φθάσει τον A (το μισό του RTT, αφού συνήθως οι δρόμοι είναι συμμετρικοί).
Έχοντας τις παραπάνω πληροφορίες, ο επιτιθέμενος προχωράει στην επόμενη
φάση της επίθεσης (εαν κάποια άλλη TCP σύνδεση έγινε σε κάποια port του A, πριν
συνεχίσει την επίθεσή του ο Z, τότε η πρόβλεψη του Z όσον αφορά το ISN θα έχει "πέσει
έξω" κατά 64,000). Συμβολίζοντας με Z(B) τον Z μεταμφιεσμένο ως B, είναι:
1 Z(B) --- SYN □ A
2 B □ SYN/ACK --- A
3 Z(B) --- ACK □ A
4 Z(B) --- PSH* □ A
Μετά το βήμα 1, όπου ζητάει σύνδεση, ο επιτιθέμενος πρέπει να αφήσει το χρονικό
περιθώριο στον A να στείλει το SYN/ACK πακέτο (ο Z δε μπορεί να το δει). Στο 3, ο
επιτιθέμενος στέλνει ένα ACK στον A, με τον *αριθμό ακολουθίας* που έχει προβλεφθεί
(συν ένα, εφόσον κάνει επιβεβαίωση).
Ανάλογα με την πρόβλεψη του επιτιθέμενου (το ACK στο βήμα 3), υπάρχουν
τρεις περιπτώσεις στην αντίδραση του A:
□ Εαν ο αριθμός ακολουθίας (sequence number) είναι ακριβώς αυτός που περίμενε το
TCP, τότε τα εισερχόμενα δεδομένα τοποθετούνται στην επόμενη διαθέσιμη θέση
στον καταχωρητή.
□ Εαν ο αριθμός ακολουθίας είναι μικρότερος από την αναμενόμενη τιμή, τα bytes
δεδομένων θεωρούνται προϊόν αναμετάδοσης και απορρίπτονται.
□ Εαν ο αριθμός ακολουθίας είναι μεγαλύτερος από την αναμενόμενη τιμή, αλλά μέσα
στα όρια του πεδίου window, τα bytes δεδομένων θεωρούνται ότι είναι bytes που
ήρθαν νωρίτερα από ότι έπρεπε, οπότε αποθηκεύονται προσωρινά από το TCP, το
οποίο περιμένει την άφιξη των bytes που υπολείπονται.

 Εαν ο αριθμός ακολουθίας είναι μεγαλύτερος από την αναμενόμενη τιμή, και έξω από
τα όρια του πεδίου window, τότε το segment απορρίπτεται, και το TCP στέλνει πίσω
ένα segment που θα αναγράφει τον *αναμενόμενο* αριθμό ακολουθίας.
Εαν έχει γίνει σωστή πρόβλεψη του ACK, τότε ο Α παραβιάζεται και μπορεί να αρχίσει η
μεταφορά των δεδομένων στο βήμα 4. Γενικά, μετά την παραβίαση, ο επιτιθέμενος
εισάγει ένα "backdoor" ("πίσω πόρτα") στο σύστημα, το οποίο θα του επιτρέψει έναν
ευκολότερο τρόπο εισβολής. Έτσι, μπορεί για παράδειγμα να χρησιμοποιηθεί η εντολή
cat ++ >> ~/.rhosts
* To PSH flag, όταν είναι αληθές, λέει στον παραλήπτη να "σπρώξει" τα δεδομένα που έχει καταχωρήσει
στην ουρά του, στην εφαρμογή, όσον το δυνατόν πιο γρήγορα.
Μέτρα πρόληψης
Μια πρώτη λύση θα ήταν η απενεργοποίηση των *r εντολών*, το σβήσιμο των
αρχείων .rhosts και των περιεχομένων του αρχείου /etc/hosts.equiv.
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 [9]. '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 αντιστοιχείστο 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 (και άλλων παρομοίων πρωτοκόλλων όπως token-ring*) 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
* δακτύλιος με κουπόνι
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 (αλλά
προφανώς διαφορετικές hardware διευθύνσεις), 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. Έτσι, για παράδειγμα, ο host που ελέγχει, μπορεί να έχει δικαίωμα NFS
πρόσβασης σε αρχεία συστημάτων άλλων hosts, rlogin πρόσβαση κ.λ.π.
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
* Είπαμε νωρίτερα ότι το σύστημα υπακούσει στην ARP cashe, μέχρις ότου αυτή εκπνεύσει. Όταν η
δεύτερη λοιπόν απάντηση φθάσει στον host, θα θεωρηθεί περιττή και θα αγνοηθεί.
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 clientserver
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,

* Ένα τμήμα δικτύου αποτελείται από ένα σύνολο μηχανών, οι οποίες μοιράζονται συσκευές και

καλωδίαση χαμηλού επιπέδου, και “βλέπουν” το ίδιο σύνολο δεδομένων στα interfaces δικτύων τους.
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 [7]:
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. Μόνο το 1996 η έκδοσή του αναβαθμίστηκε έξι φορές για λόγους ασφαλείας. Η τρέχουσα έκδοσή του είναι η V8.8.5[**] .

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.

[*] Το πρόγραμμα Crack (password cracking) είναι διαθέσιμο μέσω anonymous ftp στο: ftp://coast.cs.purdue.edu/pub/tools/unix/crack/

[**] Ανακοινώθηκε στις 21 Ιανουαρίου 1997. Ο κώδικας βρίσκεται στη διεύθυνση ftp://ftp.cs.berkeley.edu/ucb/sendmail

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 (αυτό βέβαια λύνεται με τη χρησιμοποίηση ενός HTTP proxy που θα φιλτράρει τα σχετικά πρωτόκολλα όπως απαιτείται). 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.

Άλλα standard πρωτόκολλα όπως το finger και το whois, που χρησιμοποιούνται για την ανεύρεση πληροφοριών σχετικά με άλλους χρήστες στο δίκτυο, έχουν παρουσιάσει στο παρελθόν αρκετά προβλήματα, και μηχανισμοί ασφαλείας όπως τα

firewalls τείνουν να εξαλείψουν αυτές τις υπηρεσίες. Το κύριο πρόβλημα που παρουσιάζουν, δεν είναι τόσο στις υλοποιήσεις τους, αλλά στις πληροφορίες που παρέχουν.

1.4 Ασφαλίζοντας ένα TCP/IP δίκτυο

Πολλές επιχειρίσεις σήμερα βασίζονται σε δίκτυα υπολογιστών προκειμένου να προάγουν τα συμφέροντά τους [10]. 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.

Ένα προτεινόμενο μοντέλο ασφαλείας είναι αυτό που αποτελείται από: *πολιτικές και αντικείμενα*, που δηλώνουν τους "πρωταγωνιστές του έργου", *λειτουργίες*, που καθορίζουν τί πρέπει να κάνουν οι πρωταγωνιστές, *μηχανισμοί και διαδικασίες*, που εξηγούν πώς θα το κάνουν, και τέλος *προϊόντα*, που υλοποιούν όλα τα προηγούμενα.

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 πρόληψητων 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 μαθηματικέςδιαδικασίες για την επίλυση προβλημάτων. Στο μέλλον τα
κρυπτογραφικά APIs θα καθορίζουν το πώς οι αλγόριθμοι, υλοποιημένοι σε κώδικα, θα
αλληλεπιδρούν με άλλα προγράμματα.

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 [11]. 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. Στο Παράρτημα Α, υπάρχει αναφορά σε αυτές τις πηγές.

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 [12].

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. Υπάρχει ένας μύθος που λέει ότι τα περισσότερα πλήγματα στην ασφάλεια των δικτύων προέρχονται από προικισμένους hackers που εκμεταλλεύονται "τρύπες" σε κάποιο λογισμικό (software) και παραβιάζουν υπολογιστικά συστήματα. Συνήθως όμως, η αιτία είναι τα εύκολα 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.

Έτσι, υπάρχουν προγράμματα που "υποχρεώνουν" τους χρήστες να επιλέξουν "καλά" passwords. Ένα τέτοιο πρόγραμμα είναι το npasswd.

Το πρόγραμμα npasswd*

το npasswd είναι ένα πρόγραμμα που "αναγκάζει" τα passwords να υπακούουν σε κάποια συγκεκριμένα κριτήρια προτού προστεθούν στο /etc/passwd αρχείο.Το npasswd δεν είναι ένας τυχαίος γεννήτορας συνθηματικών. Επιτρέπει στους χρήστες να επιλέξουν το password που προτιμούν αλλά πριν το επικυρώσει, κάνει τους εξής ελέγχους:

1.Συγκρίνει τα password σε αντιπαράθεση με ένα λεξικό. Εάν το password βρεθεί μέσα σε ένα λεξικό, τότε απορρίπτεται.
2.Ελέγχει αν το password αποτελείται μόνο από κεφαλαία ή μικρά γράμματα και στην περίπτωση αυτή τα απορρίπτει.
3.Ελέγχει το μέγεθος του password και εφόσον είναι μικρότερο από μία τιμή minlength ή

μεγαλύτερο από κάποια άλλη maxlength, στην πρώτη περίπτωση το απορρίπτει και στη
δεύτερη ειδοποιεί το χρήστη ότι μόνο οι maxlength χαρακτήρες χρησιμοποιούνται.
4.Απορρίπτει την επιλογή password με μη τυπώσιμους χαρακτήρες, π.χ. Control
χαρακτήρες.
5. Συγκρίνει το password με κάποιοες προσωπικές πληροφορίες όπως το login όνομα, το
όνομα του host, το όνομα και το επίθετο του χρήστη και οποιαδήποτε πληροφορία
σχετικά με το χρήστη που μπορεί να ανακτηθεί με την εντολή finger. Διάφορες
παραλλαγές αυτής της πληροφορίας, όπως π.χ η γραφή των λέξεων ανάποδα,
λαμβάνονται υπόψιν.
Εάν το password "περάσει" αυτούς τους ελέγχους, τότε εγκρίνεται και τοποθετείται στο αρχείο /etc/passwd. Όλα αυτά τα κριτήρια, ελέγχονται από τον
διαχειριστή του συστήματος διαμέσου του αρχείου /usr/adm/checkpassd.cf.
* Διαθέσιμο στη διεύθυνση ftp://coast.cs.purdue.edu/pub/tools/unix
Εκτός από το npasswd, υπάρχει και το πρόγραμμα passwd+, που κάνει παρόμοιους ελέγχους με το npasswd.
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.
Υπάρχουν συστήματα που παρέχουν συγκεκριμένους μηχανισμούς για password aging,
αλλά τα περισσότερα δεν το κάνουν. Ένας "χειρονακτικός" τρόπος κατασκευής ενός
password aging μηχανισμού από έναν διαχειριστή συστήματος είναι ο ακόλουθος:
1) Δημιουργία ενός αντιγράφου του αρχείου /etc/passwd και απόκρυψή του σε μέρος
ασφαλές από φιλόδοξους εισβολείς.

2) Μετά από 60 μέρες, σύγκριση του αντίγραφου αρχείου με το τρέχων passwd αρχείο.
Αποστολή, σε οποιοδήποτε χρήστη που δεν έχει αλλάξει το password, ενός μηνύματος
που θα τον προτρέπει να αλλάξει το password του μέσα σε 30 μέρες.
3) Τρεις εβδομάδες αργότερα, σύγκριση του αντίγραφου αρχείου με το τρέχων passwd
αρχείο. Αποστολή, σε οποιονδήποτε χρήστη που δεν έχει ακόμα αλλάξει το password,
ενός μηνύματος που θα τον προτρέπει να αλλάξει το password του μέσα σε επτά
μέρες, ή αλλοιώς θα εκδιωχθεί από το σύστημα.
4) Επανάληψη της ίδιας διαδικασίας επτά ημέρες αργότερα. Μετατροπή όλων των μη
αλλαχθέντων passwords σε αστερίσκους (*). Τα απενεργοποιημένα accounts (λογαριασμοί) δεν πρέπει να διατηρούνται στο σύστημα για πολύ καιρό, καθ'ότι είναι
αγαπημένος στόχος των εισβολέων. Πρέπει να γίνει επαφή με τους χρήστες των
ανενεργών λογαριασμών. Εαν ο χρήστης δε χρειάζεται τον λογαριασμό, τότε αυτός
καταργείται.
5) Επιστροφή στο βήμα 1 και έναρξη ενός άλλου κύκλου 90 ημερών.

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 [7]. Ένα παράδειγμα
challenge/response αυθεντικοποίησης είναι το εξής: Ο server εμφανίζει στον client ένα
string (αλφαριθμητικό). Ο client ενώνει το password του με το string που έλαβε, και

* http://www.bellcore.com/ADV-bin/jclient?page=skey.html#works

υπολογίζει την one-way hash τιμή του τελικού string. Το αποτέλεσμα του υπολογισμού αυτού, μεταδίδεται πίσω στον server. Ο server, που γνωρίζει το password του χρήστη, υπολογίσει την one-way hash τιμή με τον ίδιο τρόπο. Εαν το digest ταιριάζει με αυτό που υπολογίστικε από το χρήστη, τότε ο χρήστης αυθεντικοποιείται .**

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 [11]. 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 πιστοποιηθείη 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
** Η αυθεντικοποίηση αυτού του είδους καλείται και digest αυθεντικοποίηση.
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 [13].

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)

Σημείωση: Μια αξιόλογη μελέτη των δημοφιλών scanners ασφαλείας δικτύων, με παράθεση των πλεονεκτημάτων και μειονεκτημάτων τους, δημοσιεύεται για λογαριασμό του περιοδικού PC Week Online, στο URL: http://www.crpht.lu/CNS/html/PubServ/Security/Documents/Scanners/tdaem.html

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 **[14]**. Το πρόγραμμα έχει γραφτεί σε κώδικα C, αλλά και σε κώδικα Perl.

Επίσης, περιέχει HTML έγγραφα για τη χρήση του. Έτσι, για να τρέξει χρειάζεται έναν HTML viewer, έναν C Compiler και Perl Language έκδοση 5. 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 (perl, shell, compiled C κ.λ.π) 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" (χρησιμοποιώντας το DNS και μια γρήγορη έκδοση ενός προγράμματος τύπου Ping, ώστε να μάθει τους "ζωντανούς" στόχους), 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.
Το SATAN εκτελείται με τα δικαιώματα του root. Οι έλεγχοι που γίνονται είναι οι εξής **[15]**:
1) Εάν το σύστημα χρησιμοποιεί τον rexd.

* Τα εργαλεία αυτά είναι διαθέσιμα στη διεύθυνση ftp://coast.cs.purdue.edu/pub/tools/unix
** ftp://info.cert.org/pub/cert_advisories/CA-93:14.Internet.Security.Scanner
*** “SATAN”, περιοδικό “ΚΟΣΜΟΣ ΤΟΥ INTERNET”, τεύχος 3, σελ. 66, Αύγουστος 1995.

2) Ποιά έκδοση του sendmail χρησιμοποιείται (εκδόσεις κάτω από 8.6.10 είναι ανασφαλείς).
3) Ποιά έκδοση του anonymous ftp χρησιμοποιείται (εκδόσεις κάτω από 2.4 είναι ανασφαλείς).
4) Εάν υπάρχει modem σε πόρτα του συστήματος.
5) Βρίσκει τους τύπους των μηχανημάτων των οποίων ελέγχαι η ασφάλεια καθώς και
τους τύπους των λειτουργικών που χρησιμοποιούν και έχοντας μία λίστα με τις αδυναμίες των λειτουργικών, κοιτάει αν έχουν διορθωθεί αλλοιώς τις επισημαίνει, παραθέτοντας τον τρόπο με τον οποίο μπορούν να διορθωθούν, καθώς και που μπορούν
να βρεθούν τα σχετικά αρχεία. Παράλληλα γνωρίζει ότι ορισμένα λειτουργικά συστήματα λένε ότι διαθέτουν μία συγκεκριμένη έκδοση κάποιου προγράμματος ενώ
έχουν κάποια άλλη, π.χ. στο ULTRIX ο 4.x ftpd λέει ότι είναι έκδοσης 4.1.
6) Παραθέτει για κάθε μηχάνημα μία λίστα από υπηρεσίες που υποστηρίζονται από αυτό,
όπως NNTP, anonymous ftp, NIS, NFS, X-Windows, XDM, DNS, FTP σε μη συγκεκριμένη port.
7) Λαμβάνοντας υπόψη τα προηγούμενα αποτελέσματα ελέγχει τον mountd, rusersd,
rexd, ypserv, καθώς και την εκτέλεση εντολών από άλλα μηχανήματα χωρίς να παρέχεται
κάποιο είδος επιβεβαίωσης, όπως και το trivial ftp.

1.4.4.2 Εκτελώντας προγράμματα ελέγχου μέσα στο σύστημα

Ανάλογα με το software που είναι διαθέσιμο, και τη λειτουργικότητά του, είναι δυνατή η εκτέλεση των ελέγχων ασφαλείας, **μέσα** στο σύστημα που υπόκειται τον έλεγχο
[13]. Αυτό, για παράδειγμα, μπορεί να επιτευχθεί εαν το auditing software υποστηρίζει το
client/server μοντέλο: το server module στέλνει τις κατάλληλες εντολές στον client ώστε
να εκτελέσει επιτυχώς τον έλεγχο ορθότητας (audit) και να στείλει τα αποτελέσματα του
ελέγχου σε μια συγκεκριμένη διεύθυνση.
Το auditing software πρέπει να τοποθετείται εκτός του client συστήματος, και να διατηρείται σε ένα ασφαλές σύστημα, καθώς οι auditing ρουτίνες μπορούν εύκολα να
τροποποιηθούν ώστε να επιστρέφουν λανθασμένα αποτελέσματα.
Στα δωρεάν πακέτα* , που κυκλοφορούν στο διαδίκτυο για τους ελέγχους αυτούς,

συγκαταλέγονται και τα ακόλουθα:
 COPS
 Tiger
 Tripwire

Το σύστημα COPS

Το COPS είναι μία συλλογή από προγράμματα που το καθένα προσπαθεί να ελέγξει και μία περιοχή της ασφάλειας των UNIX μηχανημάτων **[16]**. Αναλυτικά οι έλεγχοι που γίνονται είναι οι εξής:

1) Οι άδειες (permissions, modes) για τα αρχεία, τα directories και τα devices.
* ftp://coast.cs.purdue.edu/pub/tools/unix

2) Περιεχόμενο, format και ασφάλεια των passwords και των αρχείων που ανήκουν σε
ομάδες χρηστών.

3) Τα προγράμματα και τα αρχεία που καλούνται μέσα από τα rc αρχεία (δηλαδή τα
αρχεία που διαβάζει το σύστημα κατά την εκκίνησή του) και από cron διαδικασίες.

4) Ύπαρξη root_SUID αρχείων, το κατά πόσο αυτά μπορούν να γραφούν, και το κατά
πόσο είναι προγράμματα γραμμένα σε shell.

5) CRC έλεγχος για σημαντικά binary αρχεία ή αρχεία κλειδιά για να αναφερθεί εάν
έχουν γίνει αλλαγές.

6) Εάν τα home directories, καθώς και τα αρχεία εκκίνησης των χρηστών μπορούν να
γραφούν από άλλους χρήστες. (π.χ. .cshrc, .xinitrc, .profile...)

7) Το setup του anonymous ftp.

8) Ελεύθερο tftp, decode alias στο sendmail, SUID uudecode προβλήματα, κρυμμένα shells στο inetd.conf, rexd ο οποίος τρέχει μέσα από το inetd.conf.

9) Διάφοροι έλεγχοι σχετικοί με το root -- το κύριο directory στο path του, ένα "+" στο
/etc/hosts.equiv, ελεύθερα NFS mounts, διαβεβαίωση ότι ο root είναι στο /etc/ftpusers,
κ.λ.π.

10) Αντιπαράθεση των ημερομηνιών που έχουν εκδοθεί CERT advisories με τα αρχεία
κλειδιά. Με αυτόν τον τρόπο ελέγχονται οι ημερομηνίες που αναφέρθηκαν bugs και
"τρύπες ασφαλείας" στο CERT σε αντιπαράθεση με τις ημερομηνίες δημιουργίας και
τροποποίησης των εν λόγω αρχείων. Κάποιο θετικό αποτέλεσμα δεν σημαίνει πάντα ότι
βρέθηκε bug, αλλά ότι καλό θα ήταν να κοιταχτεί το advisory για περισσότερες πληροφορίες. Κάποιο αρνητικό αποτέλεσμα, προφανώς, δεν σημαίνει ότι το λειτουργικό
δεν έχει "τρύπες", αλλά ότι έχει τροποποιηθεί κατά κάποιο τρόπο αφότου εκδόθηκε το

advisory.
Το πρόγραμμα από μόνο του αποθηκεύει τα αποτελέσματα κάτω από το directory που έχει στηθεί σε ένα νέο directory που φέρει το όνομα του μηχανήματος για το οποίο
χρησιμοποιείται το πρόγραμμα. Βλέποντας τα αποτελέσματα αυτά μπορούν να εντοπιστούν προβλήματα ασφάλειας του συστήματός και να επιλύθούν.

1.4.4.3 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 **[13]**. 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 **[15]** επεμβαίνουν μεταξύ του inetd και του προγράμματος για το οποίο έχει γίνει κλήση και να καταγράφουν το όνομα και 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 απομακρύνεταιαφού 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. Για
να εγκατασταθούν οι tcp_wrappers πρέπει να τροποποιηθεί το αρχείο /etc/inetd.conf
(αρχείο συγκρότησης του inetd) και να αλλαχθούν οι γραμμές των υπηρεσιών που
επιθυμεί ο διαχειριστής του συστήματος να ελέγχονται από το πρόγραμμα, π.χ. για το
telnet, η γραμμή
telnet stream tcp nowait root /usr/etc/telnetd telnetd
θα αλλαχθεί με τη γραμμή
telnet stream tcp nowait root /usr/local/etc/tcpd /usr/etc/telnetd
η οποία λέει στο δαίμονα inetd να τρέξει τον tcpd (δηλαδή το πρόγραμμα των wrappers)
με όνομα διεργασίας telnetd.

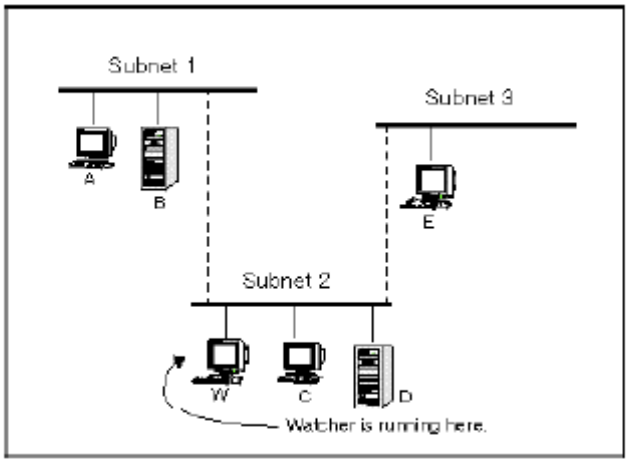
Η λειτουργία του προγράμματος καθορίζεται από τα αρχεία /etc/hosts.allow και /etc/hosts.deny. Με τη βοήθεια των αρχείων αυτών μπορεί να περιοριστεί η πρόσβαση με
βάση το host, την υπηρεσία ή συνδυασμούς. Έτσι αν ικανοποιείται κάποιος από τους
κανόνες του /etc/hosts.allow, παρέχεται η προσφερόμενη υπηρεσία σε εκείνον που τη
ζήτησε, ενώ αν ικανοποιείται κανόνας του αρχείου /etc/hosts.deny απορρίπτεται η αίτηση. Σε κάθε άλλη περίπτωση η υπηρεσία παρέχεται.

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).

* “IP-Watcher Home Page”, http://www.SecureZone.com/software/ipwatcher/index.html.



Σχήμα 6 Τοποθέτηση του IP Watcher

Σημείωση: Μια λίστα με τα περισσότερα εργαλεία για ελέγχους ασφαλείας δικτύων,
από τον οργανισμό CERT, βρίσκεται στη διεύθυνση:
ftp://info.cert.org/pub/tech_tips/security_tools.

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 **[11]**. 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 εφφικτό, 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)

Σχήμα 6 Τοποθέτηση του IP Watcher

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.

Βιβλιογραφία

[1] ANDREW S, TANENBAUM, "*Δίκτυα Υπολογιστών*", Εκδ. Παπασωτηρίου, Αθήνα 1993, σελ. 18,19,27.

[2] CRAIG HUNT, "*TCP/IP Network Administration*", O'Reilly &Associates, Inc,1995, σελ 9-15, 301-306.

[3] FARROW RIK, "*TCP SYN Flooding Attacks and remedies*", UnixWorld Online Magazine, 1995,
http://www.unixworld.com/unixworld/archives/95/security/004/004.txt.html.

[4] "*TCP SYN Flooding*", Phrack Magazine, Volume Seven, Issue Forty-Eight, July 1996, http://www.fc.net/phrack/files/p48/p48-13.html.

[5] "*TCP Flooding and IP Spoofing*", CIAC Information Bulletin, September 20, 1996, http://ciac.llnl.gov/ciac/bulletins/g-48.shtml.

[6] "*Project Loki: ICMP Tunneling*", Phrack Magazine, Volume Seven, Issue Forty-Nine, November 8 1996, hhttp://www.fc.net/phrack/files/p49/p49-06.

[7] THOMAS STEPHEN, "*Ipng and the TCP/IP Protocols*", http://fw4.iti.salford.ac.uk/ice-tel/firewall/tcpip.html.

[8] "*IP-Spoofing Demystified*", Phrack Magazine, Volume Seven, Issue Forty-Eight, June 1996, http://www.geocities.com/CapeCanaveral/3498/ipspoof.htm.

[9] ATKINS DEREK, "*Internet Security*", New Riders Publishing, 1996, σελ.258-260, 281-283, 288, 301, 303.
[10] JEFFCOATE JUDITH, "*Security in the Internet Age*", September 1997, www.westcoast.com/securecomputing/september/article/article.html#Whatare.
[11] "*RFC 1244: The Site Security Handbook*", IETF, 1995, http://www.net.ohio-state.edu/hypertext/rfc1244/toc.html
[12] BELGERS WALTER, "*Unix Passord Security*", December 6, 1993, ftp://ftp.win.tue.nl/pub/security/Unix-password-security.txt.z.
[13] DREW DALE, "*Protection of TCP/IP Based Network Elements*", 1996, http://www.security.mci.net/check.html#RTFToC12
[14] FARMER DAN, "*Improving the Security of Your Site by Breaking Into it*", 1994, http://www.trouble.org/satan/satan-demo/admin-guide-to-cracking.html.
[15] "*Checking your network security using TCP_WRAPPERS and SATAN*", NTUA Seminars, System Security: http://www.ntua.gr/seminars/sec/
[16] FARMER DANIEL, "*The COPS Security Checker System*", Purdue University, January 22, 1994, http://www.ja.net/CERT/Farmer_and_Spafford/cops.html

2
Κρυπτογραφία και Web

2.1 Εμπόριο και Internet

Η ασφάλεια της πληροφορίας συνίσταται σε τρία πράγματα: εμπιστευτικότητα (confidentiality), ακεραιότητα, (integrity) και διαθεσιμότητα (availability) των δεδομένων
[17]. 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", ως αντίβαρο στην Ηλεκτρονική Μεταβίβαση Δεδομένων (EDI) μέσω μιας μισθωμένης, ιδιωτικής γραμμής
επικοινωνίας. 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 (από συμβόλαια και τιμολόγια, έως αρχεία ήχου).
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 (in the clear), 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 **[18]**. 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:

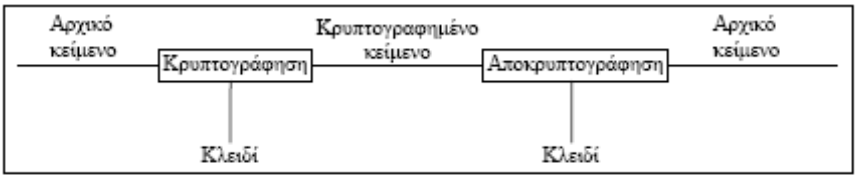
- Η Κρυπτογράφηση (**Encryption**) μετατρέπει τα δεδομένα σε μια μη αναγνώσιμη
μορφή, ώστε να εξασφαλίσει την ιδιωτικότητα (privacy). Η επικοινωνία στο Internet μοιάζει με την αποστολή μιας ευχετήριας κάρτας στην καθημερινή ζωή. Η κρυπτογράφηση προσφέρει το ψηφιακό ισοδύναμο ενός σφραγισμένου φακέλου.
- 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**, που καλείται cipher, είναι η μαθηματική συνάρτηση
που χρησιμοποιείται για την κρυπτογράφηση και την αποκρυπτογράφηση **[19]**. 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.

—

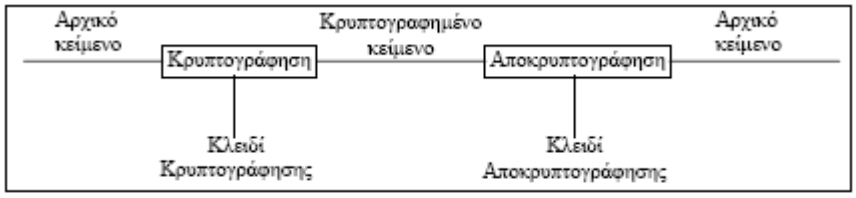


Σχήμα 1 Σύστημα μυστικού κλειδιού

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 (σχήμα2). 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

Ένα κρυπτογραφικό σύστημα, αποτελείται από τον αλγόριθμο και όλα τα πιθανά κλειδιά,
αρχικά κείμενα και κρυπτογραφημένα κείμενα.

Ταχύτητα του αλγόριθμου

Η ταχύτητα παίζει μεγάλο ρόλο στην επιλογή ενός αλγόριθμου, παρότι κανένας από αυτούς που είναι διαθέσιμοι σήμερα δεν είναι ιδιαίτερα αργός **[20]**. Τα μεγάλα
αρχεία χρειάζονται περισσότερο χρόνο για να κρυπτογραφηθούν και να αποκρυπτογραφηθούν. Τα συστήματα δημοσίου κλειδιού, παρ'ότι είναι περισσότερο
ασφαλή από τα αντίστοιχα μυστικού κλειδιού, είναι πιο "αργά" από τα δεύτερα. Συγκεκριμένα, έχει αποδειχθεί ότι οι αλγόριθμοι μυστικού κλειδιού είναι κατά μέσο όρο
10.000 φορές πιο "γρήγοροι" από τους αντίστοιχους δημόσιου κλειδιού.
Για τον παραπάνω λόγο, στην πράξη η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται για να διανείμει, κατα ασφαλή τρόπο, το μυστικό κλειδί που θα χρησιμοποιηθεί αργότερα για την επικοινωνία μέσω συμμετρικής κρυπτογράφησης. Έτσι
για παράδειγμα, ο χρήστης Α επιλέγει ένα τυχαίο κλειδί, το οποίο κρυπτογραφεί με το
δημόσιο κλειδί του χρήστη Β και στέλνει το αποτέλεσμα στον χρήστη Β. Ο χρήστης Β
αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί, και λαμβάνει το κλειδί που επέλεξε ο Α, το οποίο μπορεί να χρησιμοποιηθεί στη συνέχεια για συμμετρική κρυπτογράφηση των περεταίρω μηνυμάτων.

One-Way Hash Fuctions

Μια hash συνάρτηση συναντάται και με τις ακόλουθες ονομασίες: message digest, fingerprint, cryptographic checksum, MIC (Message Integrity Check), MDC (Message Detection Code) **[19]**. Όπως και να την ονομάσουμε, χρησιμοποιείται πάρα
πολύ συχνά στη μοντέρνα κρυπτογραφία.
Μια **hash συνάρτηση** είναι μια συνάρτηση, μαθηματική ή όχι, η οποία λαμβάνει

ως είσοδο ένα αλφαριθμητικό μεταβλητού μήκους (που καλείται προ-εικόνα) και επιστρέφει ως έξοδο ένα αλφαριθμητικό σταθερού μήκους (το οποίο καλείται hash τιμή).
Μια hash συνάρτηση θα μπορούσε να είναι μια συνάρτηση η οποία δέχεται έναν αριθμό
ΑποκρυπτογράφηΚρυπτογράφηση ση
Αρχικό
κείμενο
Κρυπτογραφημένο
κείμενο
Αρχικό
κείμενο
Κλειδί
Αποκρυπτογράφησης
Κλειδί
Κρυπτογράφησης
Σχήμα 2 Σύστημα δημόσιου κλειδιού
bytes ως είσοδο, και επιστρέφει ένα byte που ισοδυναμεί με το XOR όλων των bytes της
εισόδου.
Μια **one-way hash συνάρτηση**, είναι μια hash συνάρτηση η οποία "δουλεύει" προς μια κατεύθυνση: είναι εύκολο να υπολογίσουμε μια hash τιμή από μια συγκεκριμένη προ-εικόνα, αλλά εξαιρετικά δύσκολο να δημιουργήσουμε μια προεικόνα
η οποία έχει μια συγκεκριμένη hash τιμή. Μια "καλή" one-way hash συνάρτηση, εξασφαλίζει και την "αποφυγή συγκρούσεων" (collision-free). Δηλαδή, είναι δύσκολο να
δημιουργηθούν δύο προ-εικόνες με την ίδια hash τιμή.
Η hash συνάρτηση είναι δημόσια. Δεν υπάρχει μυστικότητα στη διαδικασία. Η ασφάλεια της στηρίζεται στη μονοδρομικότητά της. Η έξοδος (output) δεν εξαρτάται από
την είσοδο (input) κατά εμφανή τρόπο. Μια απλή αλλαγή ενός bit στην προεικόνα, αλλάζει, κατά μέσο όρο, τα μισά bits της hash τιμής. Δεδομένης μιας hash τιμής, **είναι
υπολογιστικά αδύνατο** να βρεθεί μια προ-εικόνα που να έχει αυτήν τη hash τιμή. Έτσι,
αν ο χρήστης Α θέλει να μάθει αν ο χρήστης Β έχει ένα συγκεκριμένο αρχείο, χωρίς ο
χρήστης Β να του στείλει το αρχείο, μπορεί να ζητήσει από τον Β να του στείλει τη hash
τιμή του αρχείου. Εαν ο Β στείλει την hash τιμή που υπολόγισε ο Α, τότε είναι σχεδόν
σίγουρο ότι έχει το ίδιο αρχείο.
Συνήθως, και για λόγους ταχύτητας, στην περίπτωση ψηφιακής υπογραφής ο αποστολέας υπογράφει την hash τιμή ενός κειμένου, αντί για ολόκληρο το κείμενο.
Γνωστές one-way functions είναι οι MD2, MD4, MD5 και ο Secure Hash Algorithm.
Message Authentication Code (MAC)

Ένας Κωδικός Αυθεντικοποίησης Μηνύματος ή MAC, γνωστός και ως Κωδικός Αυθεντικοποίησης Δεδομένων (Data Authentication Code) ή DAC, είναι μια one-way hash συνάρτηση με τη προσθήκη ενός μυστικού κλειδιού. Σε αυτήν την περίπτωση, το
input της συνάρτησης είναι **η προ-εικόνα και το κλειδί**. Η θεωρία είναι η ίδια όπως και
στις hash συναρτήσεις, συν το γεγονός ότι **μόνο αυτός που κατέχει το κλειδί** μπορεί να
πιστοποιήσει την hash τιμή.

2.2.1 Ασφάλεια του κρυπτογραφικού συστήματος

Η ασφάλεια ενός κρυπτογραφικού συστήματος βρίσκεται στο κλειδί του αλγόριθμου **[20]** (στους αλγόριθμους δημοσίου κλειδιού βρίσκεται στο ιδιωτικό κλειδί).
Γι'αυτόν το λόγο, οι αλγόριθμοι καθ'αυτοί δε χρειάζεται να μένουν κρυφοί. Υπάρχει μια
μεγάλη ποικιλία αλγόριθμων που διατίθεται στο Internet, και μπορούν να επιλεχθούν
ασφαλώς, αρκεί τα κλειδιά που χρησιμοποιούνται να παραμένουν μυστικά. Εαν ένα
μυστικό κλειδί γίνει γνωστό, μόνο τα μηνύματα που είναι κρυπτογραφημένα με αυτό το
κλειδί μπορούν να αποκρυπτογραφηθούν (συμμετρικός αλγόριθμος) ή τα μηνύματα που
είναι κρυπτογραφημένα με το δημόσιο κλειδί που αντιστοιχεί στο κλειδί αυτό (αλγόριθμος δημόσιου κλειδιού). Έτσι, είναι δυνατόν σε ένα δίκτυο να χρησιμοποιείται ο
ίδιος αλγόριθμος από όλους τους χρήστες του, αλλά διαφορετικά κλειδιά για κάθε χρήστη.

2.2.1.1 Μήκος κλειδιού

Αν υποθέσουμε ότι διαθέτουμε έναν "ισχυρό" κρυπτογραφικό αλγόριθμο, τότε ο μόνος τρόπος να παραβιαστεί το κρυπτοσύστημα είναι η "κατά μέτωπον επίθεση"
(**btute-force attack**) **[19]**. Σε αυτήν την επίθεση, κάποιος δοκιμάζει όλα τα πιθανά κλειδιά ώστε να βρει κάποιο που ταιριάζει με το κλειδί που χρησιμοποιήθηκε στη κρυπτογράφηση. Για να εξαπολύσει αυτού του είδους την επίθεση, ο κρυπταναλυτής
χρειάζεται ένα κρυπτογράφημα και το αντίστοιχο αρχικό κείμενο.
Η πολυπλοκότητα της παραπάνω επίθεσης υπολογίζεται εύκολα. Εαν το κλειδί έχει μήκος 8 bits, τότε υπάρχουν 2^8, ή 256 πιθανά κλειδιά. Επομένως, θα χρειαστούν 256
προσπάθειες προκειμένου να βρεθεί το σωστό κλειδί, με πιθανότητα 50% να βρεθεί το
κλειδί μετά τις μισές προσπάθειες. Εαν το κλειδί έχει μήκος 56 bits, τότε υπάρχουν 2^{56} πιθανά κλειδιά. Αν υποθέσουμε ότι ένας υπερυπολογιστής μπορεί να δοκιμάζει ένα
εκατομμύριο κλειδιά το δευτερόλεπτο, θα χρειαστεί 2285 χρόνια να βρει το σωστό

κλειδί. Σήμερα όμως, η τεχνολογία επιτρέπει την υλοποίηση τέτοιων επιθέσεων, από
πολλούς υπολογιστές που δουλεύουν παράλληλα. Έτσι, ένας pentium στα 166 MHz
μπορεί να σπάσει ένα κλειδί των 40 bits λειτουργώντας για 35 ημέρες ασταμάτητα. Το
μήκος κλειδιού πρέπει να είναι όσο το δυνατόν μεγαλύτερο.

2.2.1.2 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 (π.χ Diffie Hellman), 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 (π.χ με brute-force επίθεση) για
μεγάλο χρονικό διάστημα.

2.2.2 Κρυπτογραφικοί αλγόριθμοι που χρησιμοποιούνται στο Internet

* Για περισσότερες πληροφορίες, RFC 1750, "Randomness Recommendations for Security", http://andrew2.andrew.cmu.edu/rfc/rfc1750.html

Υπάρχει ένας μεγάλος αριθμός κρυπτογραφικών αλγορίθμων, κάθε ένας από τους
οποίους έχει τα δικά του χαρακτηριστικά, πλεονεκτήματα και μειονεκτήματα **[20]**. 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
από την προηγούμενη, καθώς παρουσιάζει αυξημένες πιθανότητες παραβίασης του
απόρρητου του μηνύματος.

2.3 Αυθεντικοποίηση με συστήματα δημόσιου και μυστικού κλειδιού

Η αυθεντικοποίηση είναι η διαδικασία πιστοποίησης ταυτότητας, ώστε κάποιος να είναι σίγουρος πως η άλλη οντότητα είναι όντως αυτή με την οποία επικοινωνεί **[21]**.

Στο ακόλουθο παράδειγμα, περιγράφουμε τον τρόπο με τον οποίο τα συστήματα δημοσίου και μυστικού κλειδιού χρησιμοποιούνται ώστε οι δύο χρήστες που επικοινωνούν να αλληλο-αυθεντικοποιούνται. Με τον συμβολισμό **{κάτι}κλειδί** εννούμε
ότι το **"κάτι"** έχει κρυπτογραφηθεί/αποκρυπτογραφηθεί με τη χρήση του **"κλειδί"**.

Ψηφιακή υπογραφή

Ας υποθέσουμε ότι η Αλίκη 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 (θα αναφερθούμε αργότερα στο πώς γίνεται αυτό). 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:

A!B τυχαίο-μύνημα

Ο Bob απαντάει κρυπτογραφώντας το μήνυμα, χρησιμοποιώντας το ιδιωτικό κλειδί του:

B!A {τυχαίο-μήνυμα} ιδιωτικό-κλειδί-Bob

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 αντικέιμενοπου 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 (αυτό σημαίνει ότι ο εκδότης του πιστοποιητικού έχει ένα πιστοποιητικό, κ.ο.κ). 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 (όπως παραπάνω, χρησιμοποιώντας ένα digest
και αποκρυπτογράφηση με δημόσιο κλειδί), 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 μηνύματοςμε 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. Το
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
A!B Ωραία Bob, να ένα μυστικό {μυστικό} δημόσιο-κλειδί-Bob
B!A { κάποιο μήνυμα } μυστικό-κλειδί

Το πώς υπολογίζεται το **μυστικό κλειδί**, εναπόκειται στην υλοποίηση του πρωτοκόλλου, αλλά θα μπορούσε απλά να είναι ένα αντίγραφο του "μυστικού"

Χρήση του MAC

Ο χρήστης Mallet δεν μπορεί να ανακαλύψει το μυστικό που αντάλλαξαν ο Bob με την Alice, αλλά μπορεί να παρεμβληθεί στην συνομιλία τους, καταστρέφοντάς την.

Αν υποθέσουμε ότι η Mallet γνωρίζει το πρωτόκολλο που χρησιμοποιούν ο Bob με την
Alice, μπορεί να συμβούν τα ακόλουθα:

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

{ digest [Alice, Εδώ Bob] } ιδιωτικό-κλειδί-Bob
A!M Ωραία Bob, να ένα μυστικό {μυστικό} δημόσιο-κλειδί-Bob
M!B Ωραία Bob, να ένα μυστικό {μυστικό} δημόσιο-κλειδί-Bob
B!M { κάποιο μήνυμα } μυστικό-κλειδί
M!A Κάτι [{ κάποιο μήνυμα } μυστικό-κλειδί]
Την περισσότερη ώρα η Mallet απλά μεταφέρει τα δεδομένα από την Alice στον Bob και τανάπαλιν. Απαξ όμως ο Bob και η Alice ανταλλάξουν ένα μυστικό, η Mallet
παρεμβάλλεται και αλλοιώνει το μήνυμα του Bob προς την Alice. Η Alice εμπιστεύεται
τον Bob ως αυτό το σημείο, οπότε θα προσπαθήσει να ενεργήσει κανονικά.επάνω σε
αυτό. Σημειώνουμε ότι η Mallet δε γνωρίζει το μυστικό, αλλά απλά μπορεί να αλλοιώσει
τα δεδομένα που είναι κρυπτογραφημένα με το μυστικό κλειδί. Η Mallet μπορεί να μην
παράγει ένα έγκυρο μήνυμα, σύμφωνα με το πρωτόκολλο, όμως μπορεί να σταθεί
τυχερή.
Προκειμένου να αποφευχθεί η ζημιά, χρησιμοποιούμε ένα MAC (Message Authentication Code) στο πρωτόκολλο (2.2.5).
MAC **:=** Digest [κάποιο μήνυμα, μυστικό]
Επειδή η Mallet δε γνωρίζει το μυστικό, δε μπορεί να υπολογίσει τη σωστή τιμή του
digest. Εαν η Mallet αλλοιώνει κατά τύχη τα δεδομένα, η πιθανότητες επιτυχίας της είναι
μικρές (υποθέτωντας ότι τα digest δεδομένα είναι μεγάλου μήκους). Έτσι, χρησιμοποιώντας π.χ το MD5 (digest αλγόριθμος), η Alice και ο Bob μπορούν να στέλνουν 128-bit MAC τιμές μαζί με τα μηνύματά τους. Η πιθανότητα της Mallet να
μαντέψει το MAC είναι μία στις 18,446,744,073,709,551,616 (δηλαδή ποτέ).
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
A!B Ωραία Bob, να ένα μυστικό {μυστικό} δημόσιο-κλειδί-Bob
B!A { **κάποιο μήνυμα, MAC** } μυστικό-κλειδί

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 **[22]**. 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.

Σήμερα, έμπιστες αρχές όπως η Verisign* εκδίδουν πιστοποιητικά, για όποιον το επιθυμεί. 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 (αυτή τη δουλειά την κάνει στην ουσία ο browser) αποδεικνύοντας την
ταυτότητά του και αποκτώντας (εαν γίνει δεκτό το πιστοποιητικό) 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 συνθματικό τους.

* (415) 961-7500, http://www.verisign.com

Σήμερα, οι δύο πιο δημοφιλείς browsers αυτην τη στιγμή, ο Netscape Communicator 4.0 και ο Internet Explorer 4.0 (που ανακοινώθηκε τον Σεπτέμβριο του
1997), ενσωματώνουν την τεχνολογία των πιστοποιητικών στις υλοποιήσεις τους. Και οι
δύο browsers, εμπιστεύονται τη Verisgn ως την έμπιστη, ανεξάρτητη αρχή που υπογράφει πιστοποιητικά. Τα πιστοποιητικά που χρησιμοποιούν οι δύο browsers, υϊοθετούν το ITU standard X.509, έκδοση 3, ένα standard για ψηφιακά πιστοποιητικά.

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.

Σημείωση: Σήμερα, ένας Web server μπορεί να αποκτήσει ένα ψηφιακό πιστοποιητικό
πολύ εύκολα*, τουλάχιστον στην Αμερική. Η εταιρία Network Solutions Inc., που διαχειρίζεται τα domains .com, .org, .edu, .gov, καθώς και καθορίζει IP διευθύνσεις σε
όλη την Αμερική, ανακοίνωσε τη συμφωνία της με την εταιρία Versign Inc. Με βάση

αυτήν τη συμφωνία, όσοι διαχειριστές δικτύων ζητούν ένα όνομα Internet domain, έχουν
το δικαίωμα να παραλάβουν και ένα ψηφιακό πιστοποιητικό για τους Web servers τους.
Έτσι, ακόμα και για έναν server που δε κάνει εμπόριο, θα υπάρχει ένα πιστοποιητικό
αποθηκευμένο και έτοιμο προς χρήση.

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 **[18]**. 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

* "Sign Up for a Digital ID Here!", by Joe Paone, LAN Times Magazine, 3/31/97, http://www.lantimes.com/97/97mar/703c014a.html

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.

2.5 Πρωτόκολλα ασφαλής επικοινωνίας στο Internet

Σήμερα υπάρχουν πολλά πρωτόκολλα που υπόσχονται ασφαλή μετακίνηση των δεδομένων μεταξύ δικτύων **[23]**. 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. Εντούτοις, υπάρχει μια θεωρία: Για
να διαλέξουν το καλύτερο πρωτόκολλο ασφαλής επικοινωνίας, οι administrators δικτύων
πρέπει να συγκρίνουν τη “λύση” με το “πρόβλημα”.

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.
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.

* http://sga.ex.ac.uk/dock/Web_docs/draft-ietf-wts-shttp-00.txt

** SSL V3.0, http://home.netscape.com/eng/ssl3/index.html

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. Έτσι, το 1995 δύο ανεξάρτητες ομάδες βρήκαν και έσπασαν τον κώδικα σε ένα RC4 40-bit κλειδί, στα
πλαίσια του SSL (V2.0) browser της Netscape, ανατρέποντας τις θεωρίες όσων πίστευαν
ότι χρειάζονται εκατομμύρια υπολογιστικών χρόνων για την παραβίαση αυτών των
προϊόντων ασφαλείας.

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** (που εξετάζεται στη συνέχεια του κεφαλαίου).

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 **[18]**. 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 (ενότητα 2.3). 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), που περιγράφεται παρακάτω.

 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.

Τί συμβαίνει κατά τη διάρκεια του SSL Handshake

Το SSL είναι σχεδιασμένο ώστε να παρέχει όσον το δυνατό διάφανες (transparent) υπηρεσίες στο χρήστη. Οι χρήστες επιλέγουν ένα link ή button που τους
συνδέει σε έναν SSL-ικανό Web server. Ένας τυπικός SSL-ικανός Web server δέχεται
αιτήσεις για SSL σύνδεση σε μια διαφορετική port (port 443 εξ'ορισμού) από αυτή των
standard HTTP αιτήσεων (port 80 εξ'ορισμού). Σημειώνουμε ότι το URL για σνδέσεις
στην port 443 είναι της μορφής: *https://www.server.com*
Όταν ο client συνδέεται σε αυτήν την πόρτα, αρχικοποιεί ένα handshake το οποίο εγκαθιστά την SSL session. Αφότου τελειώσει το handshake, η επικοινωνία κρυπτογραφείται και οι έλεγχοι ακεραιότητας εκτελούνται μέχρις ότου εκπνεύσει η SSL
session. Το SSL δημιουργεί μια session κατά τη διάρκεια της οποίας το handshake χρειάζεται να πραγματοποιηθεί μόνο μια φορά (για την πρώτη HTTP σύνδεση). Κατά τη
διάρκεια του handshake συμβαίνουν τα ακόλουθα γεγονότα:
1) Ο client και ο server ανταλλάσουν X.509 πιστοποιητικά ώστε να αποδείξουν την ταυτότητά τους. Αυτή η ανταλλαγή περιλαμβάνει προαιρετικά μια ολόκληρη αλυσίδα
πιστοποιητικών, έως το root πιστοποιητικό. Τα πιστοποιητικά ελέγχονται με βάση τους "χρόνους ζωής" των και εξετάζοντας αν το πιστοποιητικό φέρει την υπογραφή
μιας έμπιστης Αρχής Πιστοποιητικών (Certificate Authority).

2) Ο client δημιουργεί ένα τυχαίο ζεύγος κλειδιών που θα το χρησιμοποιήσει για την
κρυπτογράφηση και τον υπολογισμό των MACs. Τα κλειδιά κρυπτογραφούνται με το
δημόσιο κλειδί του server και αποστέλλονται ασφαλώς στον server.
Χρησιμοποιούνται ξεχωριστά κλειδιά για τις επικοινωνίες client-server και serverclient
(σύνολο τέσσερα κλειδιά).
3) Ένας αλγόριθμος κρυπτογράφησης και μια hash συνάρτηση (για την ακεραιότητα),
τίθενται υπό διαπραγμάτευση. Ο client παρουσιάζει μια λίστα με όλους τους αλγόριθμους που υποστηρίζει, και ο server επιλέγει τον "ισχυρότερο" αλγόριθμο που
είναι διαθέσιμος. Οι server administrators μπορούν να ενεργοποιήσουν ή να απενεργοποιήσουν συγκεκριμένους αλγόριθμους.
Η τρέχουσα έκδοση του SSL (3.0, Μάρτιος 1996) προσφέρει κάποια επιπλέον χαρακτηριστικά σε σχέση με την έκδοση 2.0 (Δεκέμβριος 1995). Ενώ οι βασικές υπηρεσίες που παρέχει το SSL (ιδιωτικότητα, ακεραιότητα και διπλή αυθεντικοποίηση)
είναι ίδιες και στις δύο εκδόσεις, η έκδοση 3.0 ενισχύει το πρωτόκολλο ως εξής:
 Λιγότερα handshake μηνύματα για γρηγορότερα handshakes
 Υποστήριξη για περισσότερους αλγόριθμους ανταλλαγής κλειδιών και κρυπτογράφησης (π.χ Diffie-Hellman, Fortezza)
 Υποστήριξη για hardware tokens (π.χ κάρτες Fortezza). Αυτό είναι και το πρώτο βήμα
για τη γενικότερη υποστήριξη των ικανών-για-κρυπτογράφηση έξυπνων καρτών.
 Βελτίωση στο πρωτόκολλο της αίτησης πιστοποιητικού. Ο server καθορίζει μια λίστα
Αρχών πιστοποιητικού (Certificate Authorities, CAs) τις οποίες εμπιστεύεται στη χορήγηση client πιστοποιητικών. Ο browser επιστρέφει ένα πρωτόκολλο υπογεγραμμένο από μία εκ των Αρχών της λίστας. Εαν δεν διαθέτει ένα τέτοιο πιστοποιητικό, το handshake αποτυγχάνει. Έτσι, ο χρήστης απαλλάσσεται από το καθήκον να διαλέξει ένα πιστοποιητικό για κάθε σύνδεση.
Το SSL σχεδιάστηκε ώστε να προστατεύει στο **επίπεδο δικτύου** ("επάνω" από το
TCP/IP και "κάτω" από το επίπεδο εφαρμογής) **[24]**. Αυτό σημαίνει ότι δεν προστατεύει
τον χρήστη από παραβιάσεις (breakins) του host στον οποίο δουλεύει. Προκειμένου να
προστατευθεί από τέτοιες παραβιάσεις, ένα πακέτο όπως το Tripwire πρέπει να συν-
λειτουργεί με το HTTPd. Το Tripwire χρησιμοποιεί "ισχυρές" hash συναρτήσεις ώστε να
βεβαιώνει ότι τα documents δεν έχουν παραλλαχθεί (από ένα χρονικό σημείο αναφοράς
και έπειτα).

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, και παρότι έχει ανακαλυφθεί από τον Ron Rivest (διακεκριμένος κρυπτογράφος), δεν έχει δοκιμαστεί αρκετά –σε σύγκριση με άλλους αλγόριθμους όπως DES ή IDEA— ώστε να είμαστε βέβαιοι για την ασφάλειά του. Η απόφαση της χρησιμοποίησης του RC4 (με κλειδί 40-bit) οφείλεται στον περιορισμό που επιβάλει η νομοθεσία των Η.Π.Α για εξαγωγή κρυπτογραφικών συστημάτων με κλειδιά μεγαλύτερα από 40 bits* .

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.

* Σήμερα, η νομοθεσία των Η.Π.Α επιτρέπει την εξαγωγή προϊόντων κρυπτογράφησης που χρησιμοποιούν κλειδιά 56 bits, αλλά υπό κάποιες προϋποθέσεις

2.5.2 Το πρωτόκολλο S-HTTP

Η βασική αυθεντικοποίηση στο πρωτόκολλο HTTP (έτσι όπως ορίζεται στην έκδοση 1.0) 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 (1994) **[23]**. 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. Έτσι, για παράδιεγμα, τα δεδομένα ενός field μιας HTML φόρμας που θα αποτελέσουν input σε
ένα cgi script και τα οποία κρίνονται εμπιστευτικά, μπορούν να κρυπτογραφηθούν (ή/και
υπογραφούν), ενώ τα υπόλοιπα δεδομένα της HTML φόρμας θα μεταφερθούν στον
server μη κρυπτογραφημένα. Έτσι, η ταχύτητα της όλης διαδικασίας είναι ικανοποιητική.
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.
Για μεγαλύτερη ταχύτητα και απόδοση, τα documents μπορούν να προ-υπογραφούν και προ-κρυπτογραφηθούν.

Υπογραφή

Για υπογραφές, ως πιθανοί αλγόριθμοι ορίζονται οι RSA και NIST-DSS **[25]**. 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 (hash του
document και ενός μυστικού κλειδιού). 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 **[26]**. 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. Η τρέχουσα έκδοση είναι η V2.0.

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 **[27]**.
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 MIME, 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 (παράγραφος 2.6), τα οποία "βασανίζονται" από την έλλειψη αλληλοσυμβατότητας (interoperability) μεταξύ των πρωτοκόλλων και των μηχανισμών
που προτείνονται κατά καιρούς από διάφορες εταιρίες **[28]**. 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,
όπως αυτή ορίζεται στα RFC 1825 εως RFC 1827* . Το IPSec υλοποιεί δύο κρυπτογραφικούς μηχανισμούς ασφαλείας για το IP:

Ο πρώτος είναι η **IP Επικεφαλίδα Αυθεντικοποίησης** (AH, ftp://ds.internic.net/rfc/rfc1826.txt), που παρέχει ακεραιότητα και αυθεντικοποίηση για τα IP
datagrams, αλλά όχι εμπιστευτικότητα (τα Ipv4 ή Ipv6 πακέτα δεν κρυπτογραφούνται).

Το AH αυξάνει επίσης τόσο το υπολογιστικό κόστος επεξεργασίας, αλλά και την υπολογιστική βραδύτητα του δικτύου. Προκειμένου να είναι συμβατά με το IPSec, όλοι
οι Ipv6-ικανοί hosts πρέπει να υλοποιούν το AH με τον MD5, έναν αλγόριθμο που παράγει ένα 128-bit digest από ένα μήνυμα οποιουδήποτε μήκους.

Ο δεύτερος μηχανισμός, το **IP Encapsulating Security Payload** (ESP, ftp://ds.internic.net/rfc/rfc1827.txt) παρέχει ακεραιότητα, αυθεντικοποίηση και

*Version 1.0, May 31, 1997, http://www.mastercard.com/set/

** Τα €?:_qWallets ("πορτοφόλια") είναι βοηθητικές εφαρμογές (helper applications) για τους browsers, αλλά
σύντομα θα ενσωματωθούν σε αυτούς, και στο μέλλον ενδεχομένως και στα λειτουργικά συστήματα.

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.
Τα AH και ESP μπορούν να χρησιμοποιηθούν μαζί ή ξεχωριστά. Πρέπει να τονιστεί, ότι
καμία από αυτές τις επικεφαλίδες (headers) δεν παρέχει προστασία από επιθέσεις *ανάλυσης επικοινωνίας*** (traffic analysis).

Κρυπτογράφηση

Ο σκοπός σχεδιασμού του IPSec είναι η εξασφάλιση ότι τόσο το Ipv4 όσο και το Ipv6 διαθέτουν ισχυρούς κρυπτογραφικούς μηχανισμούς ασφαλείας. Το πρωτόκολλο
είναι ανεξάρτητο-αλγορίθμου (algorithm independent) και επιτρέπει τη χρησιμοποίηση
standard αλγορίθμων όπως ο keyed MD5 και ο DES-CBC*** (Cipher Block Chaining). Άλλοι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται ήδη σε VPNs και έχουν
υποβληθεί σε tests αλληλλο-συμβατότητας (interperability), περιλαμβάνουν τους RC2,
RC4, IDEA και SHA.

Διαχείριση κλειδιού

* http://globecom.net/(nocl)/ietf/rfc/rfc1825.shtml, August 1995

** Επίθεση κατά την οποία παρακολουθείται η μετάδοση μηνυμάτων σε ένα δίκτυο, με σκοπό κυρίως την
αποκάλυψη της προέλευσης και του προορισμού τους, ή την αποκάλυψη του περιεχομένου τους εαν δεν
δεν έχουν κρυπτογραφηθεί.

*** Το RFC 1829, “The ESP DES-CBC Transform”, εξετάζει την υλοποίηση του DES-CBC αναφορικά με
το ESP (http://andrew2.andrew.cmu.edu/rfc/rfc1829.html).

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 sessionless 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-tohost), 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 (βλέπε 2.6) **[29]**.

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), ενώ βασίζεται σε ρουτίνες ασφαλείας που υλοποιούνται στον Windows NT Remote Access Server (RAS), συμπεριλαμβανομένου του Challenge Handshake Authentication Protocol (CHAP) και των RC4 αλγόριθμων κρυπτογράφησης (40-bit), ώστε αφενός 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

**** ftp://ftp.ietf.org/internet-drafts/draft-ietf-ipsec-isakmp-08.txt

* ftp://ftp.microsoft.com/developr/drg/pptp

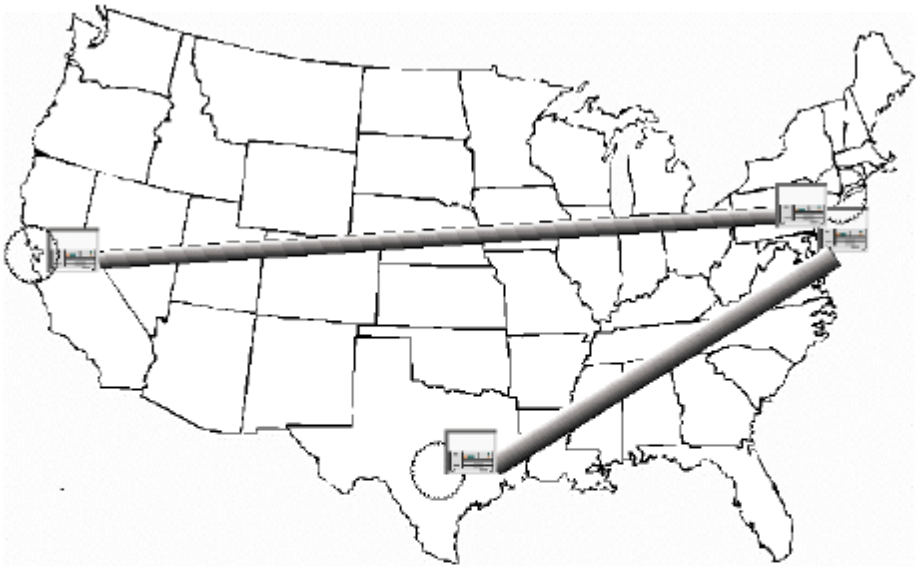
** Αυτή η "μετάφραση" πρέπει να γίνει από τον ISP. Αυτό σημαίνει, ότι ένας ISP που επιθυμείνα προσφέρει PPTP tunneling στους χρήστες του θα πρέπει να αγοράσει τμήματα εξοπλισμού από πωλητές-
εταιρίες που υποστηρίζουν το PPTP (PPTP Consortium), όπως επίσης και να ενημερώσει τον παλιότερο
εξοπλισμό με PPTP drivers.

ιδιωτικό δίκτυο ελέγχεται από έναν Windows NT server, τα πακέτα αυθεντικοποιούνται
πάλι.

Η Microsoft έχει προτείνει το PPTP στην IETF προκειμένου να γίνει standard, αλλά το πρωτόκολλο καθ'αυτό έχει ισχυρούς δεσμούς με προϊόντα της Microsoft (Windows 95/NT για client και Windows NT server), οπότε είναι δύσκολη η ευρύτερη
αποδοχή του με τα υπάρχοντα δεδομένα.
Στις αρχές του 1997***, το προτεινόμενο πρωτόκολλο της Cisco Systems incorporated **Layer 2 Forwarding** (L2F) συγχωνεύτηκε με το PPTP και έτσι προτάθηκε
στην IETF το πρωτόκολλο **Layer 2 Tunneling Protocol** (L2TP) ως Internet Draft****, το
οποίο συνδυάζει τις δυνατότητες των δύο τεχνολογιών. Η αποτελεσματικότητα του
καινούριου αυτού πρωτοκόλλου, εξετάζεται και ελέγχεται εως και αυτήν την περίοδο.

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) **[30]**.
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.

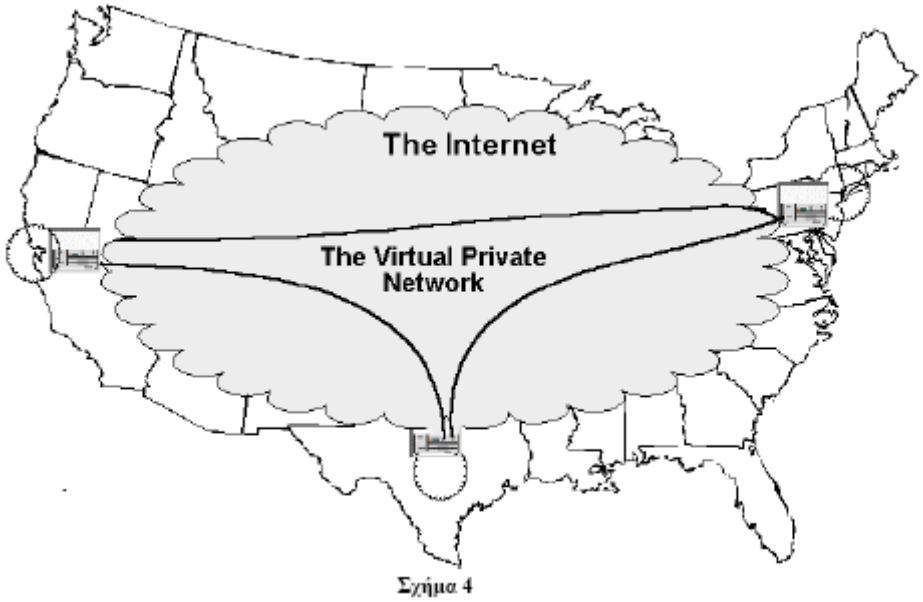


Σχήμα 3 Ένα τυπικό Ιδιωτικό Δίκτυο (PN)

*** "VPN Standards Contribute Confusion ", by Joe Paone, November 1996, LANTIMES online, http://www.lantimes.com/96nov/611a010b.html

**** http://www.masinter.net/~l2tp/ftp/draft-ietf-pppext-l2tp-04.txt

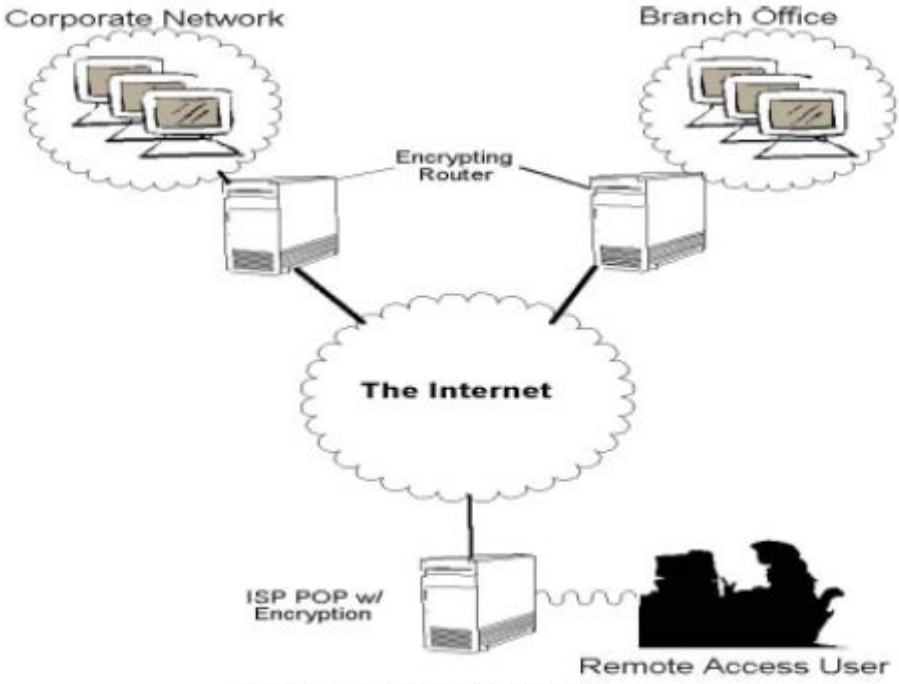
Στο παρελθόν, αλλά και σήμερα, χρησιμοποιούνταν WAN facilities όπως μισθωμένες γραμμές, ώστε να συνδέονται απομακρυσμένα sites της ίδιας εταιρίας ή συνεργαζόμενων εταιριών, όπως φαίνεται και στο σχήμα 3 που απεικονίζει ένα τυπικό PN μεταξύ τριών sites. Τονίζεται ότι για κάθε μισθωμένη γραμμή, χρησιμοποιείται 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 3,
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 4, αυτό που θα χρειάζονταν για την προσθήκη του επιπλέον
* Τοπικά δίκτυα που χρησιμοποιούν Internet-based τεχνολογία
Σχήμα 4
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 "tuunel" 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).
Επίσης, στις Η.Π.Α υπάρχουν νόμοι που απαγορεύουν την εξαγωγή προϊόντων που
προσφέρουν "ισχυρή" κρυπτογράφηση, περιορίζοντας έτσι την προοπτική για μια διεθνή
λύση.
Οι προτεινόμενες λύσεις περιλαμβάνουν πρωτόκολλα όπως το SSL, το IPSec, το PPTP, το Altavista Tunnel 97*, τα L2TP και L2F κ.α.

2.7 Ασφάλεια E-mail

Το e-mail αποτελεί ίσως τη δεσπόζουσα τεχνολογία μεταξύ των χρηστών στην κοινότητα του Internet **[31]**. 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" **[32]**. 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. Παρότι πολλά από τα gateways μεταφέρουν
δεδομένα σε S/MIME format το οποίο υποστηρίζει μεταφορά δυαδικών δεδομένων, ένας
μεγάλος αριθμός gateways εξαρτάται ακόμα από τις "πεπαλαιωμένες" τεχνολογίες του
uuencode και uudencode, που μετατρέπουν την δυαδική εικόνα σε text format για μεταφορά.
Γενικά τα gateways επεξεργάζονται τα attachments (επισυνάψεις αρχείων σε email)

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.

* Το πρωτόκολλο αυτό έχει προταθεί στην IETF και είναι υπό εξέταση. Ένα white paper που το περιγράφει
είναι στο URL: http://www.engcc.com/info/av_vpn97.html

Οι scanners είναι μια καλή αρχή, αλλά δε είναι πανάκεια. Αρχεία τα οποία προστίθενται στο e-mail μήνυμα με τη χρήση του uuencode, μπορούν να παρακάμψουν
συνήθως εύκολα τα anti-virus εκείνα προϊόντα, που ελέγχουν για δυαδικές "υπογραφές".
Όταν αργότερα ο χρήστης-παραλήπτης μετατρέψει το ASCII κείμενο σε δυαδικό, ο
"κακόβουλος" κώδικας είναι έτοιμος να εκτελεστεί.
Έτσι εξηγείται λοιπόν το πώς μια μεγάλη εταιρία-ISP, η America Online, συνέστησε στους χρήστες της να σβήνουν τα μηνύματα που προέρχονται από άγνωστους
ή ανώνυμους αποστολείς. Στην ουσία η εταιρία καταδεικνύει την αδύναμη φύση των
τεχνολογιών μεταφοράς στο Internet αλλά και την ανωριμότητα (προς το παρόν) των antvirus
προϊόντων που κυκλοφορούν στο Internet.

E-mail servers [31]

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 email
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.

* "S/MIME Central", http://www.rsa.com/smime/.

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*. Ήδη πωλητές EDI
λογισμικού και online υπηρεσιών ηλεκτρονικού εμπορίου κινούνται προς αυτήν την
κατεύθυνση.

Ανατομία του standard

Το S/MIME βασίζεται σε "ισχυρές" κρυπτογραφικές μεθόδους **[33]**.
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 (Ο RC2 αλγόριθμος υποστηρίζει κλειδιά μεταβλητού μήκους, κάτι που είναι απαραίτητο για κρυπτογράφηση μηνυμάτων εκτός
Η.Π.Α). 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** (παράγραφος 2.4). 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.
Το S/MIME χρησιμοποιεί το δημοφιλές standard πιστοποιητικού X.509, το οποίο αναπτύχθηκε από τις ISO και ITU το 1988, και σήμερα βρίσκεται στην έκδοση V3.0, η
οποία είναι αρκετά "ισχυρή" ώστε να καλύψει τις ανάγκες για παροχή πιστοποιητικών,
για αρκετά ακόμα χρόνια, σύμφωνα με τις ISO και ITU.

2.7.2 Pretty Good Privacy

Το σύστημα PGP είναι δημιουργία του P.Zimmermann και παρέχει υπηρεσίες αυθεντικοποίησης και εμπιστευτικότητας για e-mail και εφαρμογές αποθήκευσης αρχείου **[34]**.

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

* Ένας κατάλογος προϊόντων που υποστηρίζουν την τεχνολογία e-mail καθώς και τα αντίστοιχα links, είναι
διαθέσιμος στο URL: http://www.rsa.com/smime/html/products.html.

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 (δηλαδή το 128-bit MD5 μήνυμα του passphrase) 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 MD5 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 τοκλειδί 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.

Διαχείριση δημόσιου κλειδιού

Το σύστημα PGP χρησιμοποιεί διάφορες προσεγγίσεις για την ελαχιστοποίηση του κινδύνου το αρχείο δημόσιου κλειδιού ενός χρήστη να περιέχει κάλπικα δημόσια
κλειδιά. Συγκεκριμένα, εαν ο χρήστης Α θέλει να αποκτήσει ένα αξιόπιστο δημόσιο
κλειδί για τον χρήστη Β, μπορεί να ακολουθήσει μια από τις ακόλουθες προσεγγίσεις:

- Ο Α παραλαμβάνει το δημόσιο κλειδί του Β με φυσικό τρόπο δηλαδή ο Β καταχωρεί
το δημόσιο κλειδί του σε μια δισκέτα και στη συνέχεια την παραδίδει στον Α.
- Επαλήθευση του κλειδιού μέσω τηλεφωνικής κλήσης. Ένας εναλλακτικός πιο πρακτικός τρόπος είναι αυτός της αποστολής του κλειδιού με e-mail. Δηλαδή, ο Α θα
μπορούσε να έχει ένα 128-bit MD5 αριθμό του κλειδιού δεκαεξαδικής μορφής που
δημιουργεί το PGP, γνωστή ως “δακτυλικό αποτύπωμα του κλειδιού” (fingerprint).
Στη συνέχεια ο Α τηλεφωνεί στον Β και του ζητάει να υπαγορεύσει την κωδικοποιημένη αυτή μορφή. Εαν οι δυο αυτές κωδικοποιημένες μορφές ταιριάζουν
επιτυγχάνεται η επαλήθευση του κλειδιού.
- Απόκτηση του δημόσιου κλειδιού του Β από μια αμοιβαίως έμπιστη οντότητα D. Για
τον σκοπό αυτόν η έμπιστη οντότητα D δημιουργεί ένα υπογεγραμμένο πιστοποιητικό
(signed certificate) το οποίο περιέχει το δημόσιο κλειδί του Β, το χρόνο δημιουργία
του και τη διάρκεια ισχύος του. Στη συνέχεια, η οντότητα D δημιουργεί ένα MD5 μήνυμα του πιστοποιητικού, το κρυπτογραφεί με το ιδιωτικό της κλειδί και προσαρτά
σε αυτό την υπογραφή της. Το υπογεγραμμένοπιστοποιητικό μπορεί να αποσταλεί
στον Α είτε μέσω του Β είτε απευθείας από την οντότητα D.
- Απόκτηση του δημόσιου κλειδιού του Β από μια έμπιστη αρχή πιστοποίησης. Πάλι,
δημιουργείται ένα πιστοποιητικό δημόσιο κλειδιού υπογεγραμμένο από την αρχή έκδοσης. Στη συνέχεια, ο Α μπορεί να προσπελάσει την αρχή παρέχοντας το όνομά
του και να παραλάβει το υπογεγραμμένο πιστοποιητικό.
- Απόκτηση του δημόσιου κλειδιού του Β από ένα key-server και επαλήθευση του
δακτυλικού αποτυπώματος είτε άμεσα από τον Β είτε παρακολουθώντας τη δημόσια
μετάδοση του Β.

2.7.3 PGP εναντίον S/MIME

Το 1991 Ο P. Zimmerman έγραψε το πρόγραμμα PGP για κρυπτογράφηση e-mail
[35], 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 (PGP Inc.) 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 4.0 όσο και
ο Microsoft Explorer 4.0* υποστηρίζουν την τεχνολογία S/MIME για την κρυπτογράφηση των e-mail μηνυμάτων.
Σήμερα λοιπόν εξελίσσεται ένας από τους “θρησκευτικούς” πολέμους για τους οποίους φημίζεται η βιομηχανία υπολογιστών. Από τη μία, υπάρχει μια συμμαχία μεταξύ
των Netscape, Microsoft, RSA Data Security** και άλλων εταιριών, που προωθούν το
S/MIME με σκοπό να γίνει το παγκοσμίως αποδεκτό e-mail standard. Από την άλλη,
υπάρχει η PGP Inc, η οποία ισχυρίζεται ότι το S/MIME standard είναι εκ φύσεως “αδύναμο”, επειδή υποστηρίζει κρυπτογράφηση με κλειδί 40-bit, που δεν προσφέρει
ασφάλεια (αλλά μπορεί να εξαχθεί από τις Η.Π.Α σύμφωνα με τη νομοθεσία τους).
Για το S/MIME το πρόβλημα δεν είναι το PGP, αλλά η IETF (Internet Engineering Task Force). Συγκεκριμένα, η RSA έχει προτείνει εδώ και καιρό το S/MIME
ως standard, αλλά η IETF έχει διατυπώσει ορισμένες ενστάσεις:
1) Πρώτον, το S/MIME είναι trademark της RSA Data Security. Για να γίνει standard, η
RSA Data Security θα πρέπει να εγκαταλείψει το trademark.
2) Το S/MIME standard προς το παρόν απαιτεί κρυπτογράφηση και κρυπτογράφηση με
τους αλγόριθμους RC2 και RSA. Ο RC2 αλγόριθμος όμως, αποτελεί μονοπώλιο της
RSA Data Security, η οποία έχει απειλήσει με μηνύσεις όποιον χρησιμοποιήσει τον
αλγόριθμο χωρίς την άδειά της.
3) Τέλος, η IETF βλέπει με αρκετή δυσπιστία την κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων με κλειδί 40-bit, ώστε να το καθιερώσει ως standard.

* Ο Microsoft Explorer 4.0 συνοδεύεται από το πρόγραμμα Microsoft Outlook Express για αποστολή και
λήψη e-mail μηνυμάτων.
** Η RSA Data Security ανέπτυξε την τεχνολογία S/MIME.
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.
Σημείωση: Ο Bruce Schneier, συγγραφέας του βιβλίου “Applied Cryptography”, δημιούργησε ένα Windows 95 Screensaver, το οποίο **“σπάει” κρυπτογραφημένα email**
μηνύματα, τα οποία έχουν κρυπτογραφηθεί με τον Netscape Navigator ή τον Microsoft
Explorer που χρησιμοποιούν την τεχνολογία S/MIME (με κλειδί 40-bit)***. “Κατά μέσο
όρο απαιτούνται 35 ημέρες σε έναν Pentium 166 MHz”, δήλωσε ο Schneier. Η πραγματική δύναμη του προγράμματος που έγραψε ο Schneier, είναι ότι σχεδιάστηκε
ώστε δουλεύει σε πολλές μηχανές, παράλληλα συνδεδεμένες σε ένα τοπικό δίκτυο.
Συγκεκριμένα, 12 μηχανήματα μπορούν να “σπάσουν” το μήνυμα σε λιγότερες από τρεις
μέρες, ενώ 1000 μηχανήματα μπορούν να “σπάσουν” το μήνυμα σε 50 λεπτά. Το πρόγραμμα, το οποίο λειτουργεί ως screensaver, ψάχνει για μεγάλους πρώτους αριθμούς,
και είναι διαθέσιμο στο Web site του Schneier από τις 27 Σεπτεμβρίου 1997.

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 (ο server εφαρμογής, ή απλά server)
χωρίς να στέλνει στο δίκτυο δεδομένα που θα επέτρεπαν σε έναν hacker ή στον πιστοποιητή να παραστήσουν το υποκείμενο **[36]**. Το Kerberos παρέχει προαιρετικά
ακεραιότητα και εμπιστευτικότητα για δεδομένα που μεραφέρονται από τον client στον
server. Το Kerberos αναπτύχθηκε στα μέσα της δεκαετίας του 80’ ως τμήμα του προγράμματος Athena του MIT. Καθώς η χρήση του εξαπλώθηκε και σε άλλα περιβάλλοντα, σημειώθηκαν κάποιες αλλαγές στο σύστημα, ώστε να υποστηρίζονται
ποικίλες πολιτικές και μοντέλα χρήσης. Έτσι, ο σχεδιασμός του Kerberos έκδοση V5
άρχισε το 1989. Παρότι η έκδοση 4 υπάρχει ακόμα σε αρκετά sites, η έκδοση 5 θεωρείται
ως το standard Kerberos.

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**

*** "S/MIME Cracked by a Screensaver", by Simson Garfinkel, 26 Σεπτεμβρίου 1997, Wired Magazine, http://www.wired.com/news/news/technology/story/7220.html.

* RFC 1510

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

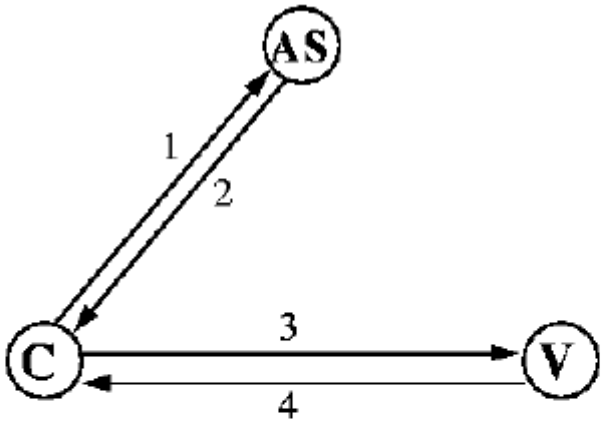
Ο client και ο server δεν μοιράζονται εξαρχής ένα κλειδί κρυπτογράφησης. Όποτε ένας client αυθεντικοποιεί τον εαυτό του σε έναν καινούριο πιστοποιητή, βασίζεται στο
ότι ο server αυθεντικοποίησης θα δημιουργήσει ένα καινούριο κλειδί κρυπτογράφησης
και θα το διανείμει ασφαλώς στα δύο μέρη. Αυτό το καινούριο 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 περιλαμβάνειτο 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: $\{K_{c,v}, v, time_{exp}, n, ...\}K_c$, $\{T_{c,v}\}K_v$
3. ap_req: $\{ts,ck, K_{subsession}, ...\}K_{c,v}$ $\{T_{c,v}\}K_v$
4. ap_rep: $\{ts\}K_{c,v}$ (optional)

$T_{c,v} = K_{c,v}, c, time_{exp}$ ...

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. Εαν 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
Σχήμα 6 Βασικό πρωτόκολλο αυθεντικοποίησης στο kerberos (απλοποιημένο)
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.

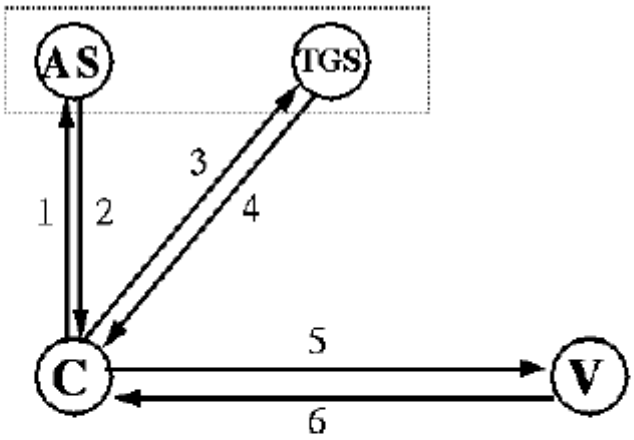
Αίτηση Αυθεντικοποίησης και απάντηση

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 6 (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.

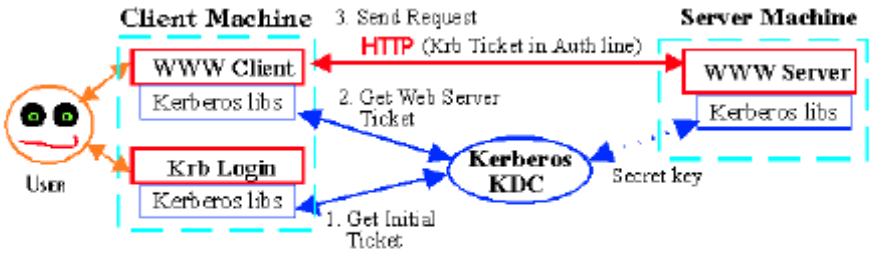


1. as_req: c, tgs, $time_{exp}$, n
2. as_rep: $\{K_{c,tgs}, tgs, time_{exp}, n, ...\}K_c$, $\{T_{c,tgs}\}K_{tgs}$
3. tgs_req: $\{ts, ...\}K_{c,tgs}$ $\{T_{c,tgs}\}K_{tgs}$, v, $time_{exp}$, n
4. tgs_rep: $\{K_{c,v}, v, time_{exp}, n, ...\}K_{c,tgs}$, $\{T_{c,v}\}K_v$
5. ap_req: $\{ts, ck, K_{subsession},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

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 (mutual-authentication) 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 **[37]**. 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

Στη συνέχεια παρατίθεται ένα παράδειγμα του πρωτοκόλλου που χρησιμοποιείται: στο παράδειγμά μας, ο browser είναι ο Mosaic της NCSA και ο Web
server είναι ο httpd 1.3.
1. Ο client στέλνει την αρχική αίτηση (ή, αν μπορεί ματαβαίνει απευθείας στο βήμα 3):
GET /restricted/adam.html HTTP/1.0
Accept: */*
User-Agent: NCSA Mosaic for the X Window System/2.4 libwww/2.12 modified
2. Ο server βλέπει ότι απαιτείται αυθεντικοποίηση, οπότε στέλνει ένα μήνυμα 401:
HTTP/1.0 401 Unauthorized
Date: Friday, 03-Feb-95 18:45:13 GMT
Server: NCSA/1.3
MIME-version: 1.0
Content-type: text/html
WWW-Authenticate: KerberosV4
3. Ο client παίρνει ένα εισητήριο για τον server, και ξανα-υποβάλλει την αίτηση εισαγάγοντας σε αυτήν το εισητήριο που πήρε:
GET /restricted/adam.html HTTP/1.0
Accept: */*
User-Agent: NCSA Mosaic for the X Window System/2.4 libwww/2.12 modified
Authorization: KerberosV4 acain 0406004e4353412e554955
32e454455003820c3e4fc931b68ed20d0f696ee74148a696eb4
3694ee91e5623b953a5dfd3be00642596ff846
4. Ο server απαντά με το έγγραφο, και το κρυπτογραφημένο timestamp+1 ώστε να αυθεντικοποιήσει τον εαυτό του:
HTTP/1.0 200 OK
Date: Friday, 03-Feb-95 18:45:16 GMT
Server: NCSA/1.3
MIME-version: 1.0
Content-type: text/html
Last-modified: Wednesday, 04-Jan-95 22:58:20 GMT
Content-length: 624
WWW-Authenticate: KerberosV4 [c3602905a92b683f] User authenticated
HTML document

Βιβλιογραφία

[17] COBB CHEY, "*Security Issues in Internet Commerce*", NCSA White Paper, 1996, http://www.ncsa.com/library/inetsec2.html.
[18] "*Securing Communications on the Intranet and over the Internet*", Netscape Corporation, July 1996, http://home.netscape.com/newsref/ref/128bit.html.
[19] SCHNEIER BRUCE, "*Apllied Cryptography*", John Wiley & Sons, Inc., σελ.2-5, 29-33, 151.
[20] DIANE E. LEVINE, "*Shielding the LAN*", InfoSecurity Magazine, February 1997, http://www.bitwise.net/isn/articles/9702/article2.htm.
[21] "*Using RSA Public Key Cryptography*", Netscape Corporation, http://home.netscape.com/newsref/ref/rsa.html.
[22] RADOSEVICH LYNDA, "*Digital Certification goes well beyond password*", InfoWorld Magazine, July 28, 1997, http://www.cio.com/WebMaster/0796_retail_1.html.
[23] BRADLEY F. SHIMMIN, "*Internet Security Protocols: Oxymoron or Solution?*", LAN TIMES Online, November 1996, http://www.lantimes.com/96nov/6116058a.html.
[24] SHSTACK ADAM, "*An Overview of SSL (version 2)*", May 1995, http://web.homeport.org/~adam/ssl.http.
[25] LIPP PETER, "*Security Concepts for the WWW*", 1996, σελ. 91-92.
[26] "*The Private Communication Technology Protocol*", Internet-Draft, version 2.0, April 1996, http://sectest.microsoft.com/pct/pct2.html.
[27] GARFINKEL SIMSON, "*Is the Web Set for SET*?", HotWired Magazine, 1997, http://www.hotwired.com/packet/packet/96/47/index2a.html.
[28] AUSTIN TOM, "*Tunnel Vision*", InfoSecurity Magazine, May 1997, http://www.infosecnews.com/articles/9705/article5.html.
[29] FOGARTY KEVIN, "*Microsoft tunnels the 'Net' with new protocol*", Network World Magazine, http://www.nwfusion.com/netresources/1013current.html.
[30] "*Virtual Private Networks*", http://telecommunity.nynexst.com/irl/source/vpn.html.
[31] WILLIAM P.DOWNS, "*Just Between Us: Encryption and Email*", InfoSecurity News Magazine, June 1997, http://www.infosecnews.com/articles/9706/article3.html.
[32] MERENBLOOM PAUL, "*Watch out for the threat of E-mail viruses*", LAN TIMES Online, June 1997, http://www.lantimes.com/lantimes/97/97jun/706a007a.html.
[33] DUSSI STEVE, "*S/MIME: Anatomy of a Secure E-mail Standard*", RSA Data Security Inc., http://www.ema.org/html/pubs/mmv2n4/s-mime.html.
[34] ΧΡΥΣΙΚΟΠΟΥΛΟΣ Β., "*Ασφάλεια Πληροφοριακών Συστημάτων*", Σημειώσεις διδασκαλίας, Πειραιάς 1997, σελ.66-71
[35] GARFINKEL SIMSON, "*Pretty Good Politics*", Wired Magazine, May 7, 1997, http://www.wired.com/news/news/technology/story/3659.html.
[36] NEUMAN CLIFFORD, "*Kerberos: An Authentication Service for Computer Networks*", IEEE, 1994, http://nii.isi.edu/publications/kerberos-neuman-tso.html.
[37] CAIN ADAM, "*Tutorial on Security, Authentication, and Privacy on the Web*", May 6, 1996, http://www5conf.inria.fr/fich_html/slides/tutorials/T1/index.html.