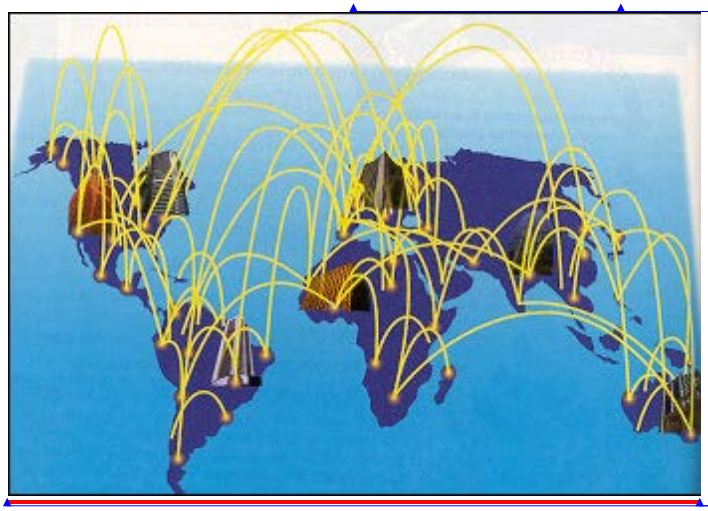
Τ. Ε. Ι. ΗΠΕΙΡΟΥ **ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ (Σ. Δ. Ο)**

T. E. I. OF EPIRUS **SCHOOL OF MANAGEMENT AND ECONOMICS**

DEPARTMENT OF COMMUNICATIONS, INFORMATICS AND MANAGEMENT

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ : «Ασφάλεια στο Διαδίκτυο»



ΕΚΠΟΝΗΣΗ ΕΡΓΑΣΙΑΣ:
ΓΚΡΙΖΗΣ ΝΙΚΟΛΑΟΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ :
ΤΣΙΑΝΤΗΣ ΛΕΩΝΙΔΑΣ

ΑΡΤΑ 2006

Formatted: Top: 1,59 cm, Bottom: 1,9 cm
Formatted: English (U.K.)
Formatted: English (U.K.)
Formatted: English (U.K.)
Formatted: English (U.K.)
Formatted: English (U.K.)
Formatted: English (U.K.)
Formatted: Font: 14 pt, English (U.K.)
Formatted: English (U.K.)
Formatted: English (U.K.)
Formatted: English (U.K.)
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Centered
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 24 pt, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Centered
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

ΠΕΡΙΕΧΟΜΕΝΑ

Formatted …
Formatted …
Formatted …
Formatted …
Formatted …
Formatted …
Formatted …
Formatted: Bullets and Numbering
Formatted …
Formatted …
Formatted …
Formatted …
Formatted: Bullets and Numbering
Formatted …
Formatted: Bullets and Numbering
Formatted …
Formatted …
Formatted …
Formatted …
Formatted …
Formatted …
Formatted …
Formatted …
Formatted: Bullets and Numbering
Formatted …
Formatted: Right: 0,63 cm

[Στοιχεία από βιβλίο «Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο internet» του Douglas Comer]

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, No underline

Formatted: Indent: Left: 0,63 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

ΕΙΣΑΓΩΓΗ

Formatted: Font: (Default) Arial, 14 pt, Bold

Formatted: Font: (Default) Arial

Αύξηση δικτύωσης των υπολογιστών

Formatted: Indent: First line: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Τα δίκτυα των υπολογιστών αυξάνονται εκρηκτικά. Πριν από δύο δεκαετίες, ελάχιστοι είχαν πρόσβαση σε ένα δίκτυο. Σήμερα η επικοινωνία των υπολογιστών έχει γίνει απαραίτητο μέρος της υποδομής μας. Η δικτύωση χρησιμοποιείται σε κάθε δραστηριότητα των επιχειρήσεων, όπως την διαφήμιση, την παραγωγή, τη διεκπεραίωση, το σχεδιασμό, την κοστολόγηση, και τη λογιστική. Γι' αυτό οι περισσότερες εταιρείες έχουν πολλά δίκτυα. Πολλά σχολεία σε όλες τις βαθμίδες, από τη στοιχειώδη μέχρι τη μεταπτυχιακή εκπαίδευση, χρησιμοποιούν δίκτυα υπολογιστών για να παρέχουν στους διδασκόμενους και τους διδάσκοντες άμεση πρόσβαση σε πληροφορίες που υπάρχουν σε ηλεκτρονικές βιβλιοθήκες σε όλον τον κόσμο. Δίκτυα χρησιμοποιούν οι κρατικές, περιφερειακές και οι τοπικές δημόσιες υπηρεσίες, καθώς και οι στρατιωτικοί οργανισμοί. Με μια φράση, τα δίκτυα υπολογιστών είναι παντού.

Η συνεχιζόμενη ανάπτυξη του παγκόσμιου διαδικτύου, του internet, είναι ένα από τα πιο ενδιαφέροντα και εντυπωσιακά φαινόμενα της δικτύωσης. Πριν από είκοσι χρόνια, το internet ήταν ένα ερευνητικό έργο που περιλάμβανε μερικές δεκάδες τοποθεσίες. Σήμερα, έχει εξελιχθεί σε ένα σύστημα επικοινωνίας που χρησιμοποιείται στην παραγωγή, το οποίο φτάνει σε εκατομμύρια άτομα από όλες τις κατοικημένες χώρες του κόσμου. Στις Ηνωμένες Πολιτείες, το internet συνδέει εταιρείες, κολέγια και πανεπιστήμια, καθώς και κρατικές, περιφερειακές και οι τοπικές δημόσιες υπηρεσίες και

Formatted: Right: 0,63 cm

σχολεία. Ακόμα, οι ιδιωτικές κατοικίες έχουν πρόσβαση χαμηλής ταχύτητας στο internet μέσω του τηλεφωνικού συστήματος και πρόσβαση υψηλής ταχύτητας μέσω καλωδιακών μόντεμ, δορυφόρων, DSL, και ασυρμάτων τεχνολογιών. Αποδείξεις για τις επιπτώσεις του internet στην κοινωνία μπορούμε να δούμε στις διαφημίσεις των περιοδικών και της τηλεόρασης, οι οποίες περιέχουν παραπέμπουν σε ιστοσελίδες του internet με πρόσθετες πληροφορίες για τα προϊόντα και τις υπηρεσίες των διαφημιζόμενων προϊόντων.

Η μεγάλη αύξηση της δικτύωσης έχει και οικονομικές συνέπειες. Τα δίκτυα μετάδοσης δεδομένων έχουν κάνει εφικτές τις συναλλαγές από απόσταση για μεμονωμένα άτομα και έχουν αλλάξει τις επαγγελματικές επικοινωνίες. Ακόμα, έχει αναδυθεί μια ολόκληρη βιομηχανία η οποία αναπτύσσει δικτυακές τεχνολογίες, προϊόντα, και υπηρεσίες. Η δημοτικότητα και σημασία της δικτύωσης υπολογιστών έχει δημιουργήσει σε όλες τις εργασίες ισχυρή ζήτηση για άτομα με περισσότερες γνώσεις δικτύωσης. Οι εταιρείες χρειάζονται άτομα που να μπορούν να σχεδιάζουν, να προμηθεύονται, να εγκαθιστούν, να λειτουργούν και διαχειρίζονται τα συστήματα υλικού και λογισμικού που αποτελούν τα δίκτυα και τα διαδίκτυα υπολογιστών. Ακόμα, ο προγραμματισμός υπολογιστών δεν περιορίζεται πλέον σε μεμονωμένους υπολογιστές. Αναμένεται από τους προγραμματιστές να χρησιμοποιούν λογισμικό εφαρμογών που να μπορεί να επικοινωνεί με λογισμικό που βρίσκεται σε άλλους υπολογιστές.

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

~~(37)ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ~~

Formatted: Font: (Default) Arial

~~37.2 (από βιβλίο)~~

~~ΑΣΦΑΛΗ ΔΙΚΤΥΑ ΚΑΙ ΠΟΛΙΤΙΚΕΣ~~

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0 cm, Line spacing: 1,5 lines

ΚΕΦΑΛΑΙΟ 1

Formatted: Font: (Default) Arial, Bold

ΣΥΝΤΟΜΗ ΑΝΑΦΟΡΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Formatted: Font: (Default) Arial, Bold

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

Τι είναι ένα ασφαλές δίκτυο; Μπορεί ένα διαδίκτυο να γίνει ασφαλές; Αν και η έννοια του ασφαλούς δικτύου (secure network) γοητεύει τους περισσότερους χρήστες, τα δίκτυα δεν μπορούν να ταξινομηθούν απλώς σε ασφαλή και μη ασφαλή, επειδή ο όρος αυτός δεν είναι απόλυτος – κάθε οργανισμός ορίζει ένα επίπεδο πρόσβασης που επιτρέπει ή απαγορεύει -. Για παράδειγμα, μερικοί οργανισμοί αποθηκεύουν δεδομένα τα οποία είναι πολύτιμα. Οι οργανισμοί αυτοί ορίζουν ως ασφαλές δίκτυο ένα σύστημα που εμποδίζει τους ξένους να αποκτούν πρόσβαση στους υπολογιστές του οργανισμού. Άλλοι οργανισμοί χρειάζεται να κάνουν τις πληροφορίες γνωστές στους ξένους, αλλά να μην τους επιτρέπουν να κάνουν αλλαγές στα δεδομένα. Οι οργανισμοί αυτοί μπορεί να ορίσουν ως ασφαλές ένα δίκτυο το οποίο επιτρέπει απεριόριστη πρόσβαση στα δεδομένα, αλλά περιλαμβάνει μηχανισμούς που εμποδίζουν τις αλλαγές από αναρμόδιους. Άλλες ομάδες πάλι, εστιάζουν την προσοχή τους στο να διατηρούν τις επικοινωνίες εμπιστευτικές. Αυτές ορίζουν ως ασφαλές ένα δίκτυο στο οποίο κανένας άλλος εκτός από τον τελικό αποδέκτη δεν μπορεί να υποκλέψει και να διαβάσει ένα μήνυμα. Τέλος, πολλοί μεγάλοι οργανισμοί χρειάζονται έναν σύνθετο ορισμό της ασφάλειας, που να επιτρέπει την πρόσβαση σε κάποια επιλεγμένα δεδομένα ή υπηρεσίες που έχει επιλέξει ο οργανισμός να κάνει δημόσια, ενώ εμποδίζει την πρόσβαση ή την τροποποίηση των ευαίσθητων δεδομένων και υπηρεσιών τα οποία διατηρούνται εμπιστευτικά.

Επειδή δεν υπάρχει απόλυτος ορισμός του ασφαλούς δικτύου, το πρώτο βήμα που πρέπει να κάνει ένας οργανισμός για να πετύχει ένα ασφαλές σύστημα είναι να ορίσει την πολιτική ασφαλείας (security policy) του. Η πολιτική αυτή δεν καθορίζει πως θα επιτευχθεί η προστασία. Καθορίζει όμως ρητά και με σαφήνεια τα στοιχεία που πρέπει να προστατεύονται.

Formatted: Font: (Default) Arial, Greek

Ο ορισμός μιας πολιτικής ασφάλειας δικτύου είναι σύνθετη δουλειά. Η πολυπλοκότητα οφείλεται κυρίως στο ότι μια πολιτική ασφάλειας που ισχύει για τα υπολογιστικά συστήματα που είναι συνδεδεμένα στο δίκτυο. Ειδικότερα, ο ορισμός μιας πολιτικής για τα δεδομένα που περνούν από ένα δίκτυο δεν εγγυάται ότι τα δεδομένα θα είναι ασφαλή. Για παράδειγμα, ας υποθέσουμε ότι κάποια αρχεία είναι αποθηκευμένα σε ένα αρχείο που επιτρέπεται η ανάγνωσή του. Η ασφάλεια του δικτύου δεν μπορεί να εμποδίσει τους αναρμόδιους χρήστες που έχουν λογαριασμό στον υπολογιστή να πάρουν ένα αντίγραφο των δεδομένων. Επομένως για να είναι αποτελεσματική μια πολιτική ασφαλείας, πρέπει να ισχύει πάντοτε. Η πολιτική

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

πρέπει να ισχύει για τα δεδομένα που είναι αποθηκευμένα σε δίσκο, για τα δεδομένα που μεταφέρονται μέσω τηλεφωνικής γραμμής με ένα μόντεμ, για τις πληροφορίες που τυπώνονται σε χαρτί, για τα δεδομένα που μεταφέρονται σε φορητά μέσα, όπως μια δισκέτα, και για τα δεδομένα που μεταφέρονται μέσω ενός δικτύου υπολογιστών.

Η εκτίμηση του κόστους και της ωφέλειας των διαφόρων πολιτικών ασφαλείας κάνει επίσης το ζήτημα πιο σύνθετο. Συγκεκριμένα, μια πολιτική ασφαλείας δεν μπορεί να οριστεί παρά μόνο αν ο οργανισμός αντιληφθεί την αξία των πληροφοριών του. Σε πολλές περιπτώσεις η αξία των πληροφοριών είναι δύσκολο να εκτιμηθεί. Φανταστείτε λοιπόν, για παράδειγμα, μια απλή βάση δεδομένων μισθοδοσίας, η οποία περιέχει μια εγγραφή για κάθε υπάλληλο, τις ώρες που εργάστηκε ο υπάλληλος, και την αμοιβή του. Η ευκολότερη άποψη της αξιολόγησης είναι να εκτιμηθεί το κόστος αντικατάστασης. Δηλαδή μπορεί να υπολογιστούν οι ώρες εργασίας που χρειάζονται για να ξαναδημιουργηθεί ή να επαληθευθεί το περιεχόμενο της βάσης δεδομένων (π.χ. με την αποκατάσταση των δεδομένων από ένα εφεδρικό αντίγραφο ή με την πραγματοποίηση της εργασίας που χρειάζεται για να συλλεχθούν οι πληροφορίες). Μια δεύτερη άποψη της αξιολόγησης είναι ~~8~~ να εκτιμηθεί το παθητικό που μπορεί να προκληθεί στον οργανισμό αν οι πληροφορίες είναι λανθασμένες. Για παράδειγμα αν ένα αναρμόδιο άτομο αυξήσει τις αμοιβές σε μια βάση δεδομένων μισθοδοσίας, η εταιρία θα μπορούσε να επιβαρυνθεί με οποιοδήποτε κόστος αν οι υπάλληλοι θα πληρώνονταν περισσότερο. Μια τρίτη άποψη της αξιολόγησης είναι το έμμεσο κόστος που θα μπορούσε να προκληθεί από παραβιάσεις της ασφάλειας. Για παράδειγμα, αν οι πληροφορίες μισθοδοσίας κοινοποιηθούν, μπορεί οι ανταγωνιστές να επιλέξουν να προσλάβουν κάποιους εργαζόμενους, με αποτέλεσμα ένα κόστος πρόσληψης και εκπαίδευσης αντικαταστατών, καθώς και αυξήσεις αμοιβών για να κρατήσει η εταιρία κάποιους υπαλλήλους.

Μιλώντας γενικά, πρέπει να τονίσουμε ότι η επινόηση μιας πολιτικής ασφάλειας δικτύου μπορεί να είναι σύνθετη δουλειά, επειδή μια λογική πολιτική απαιτεί να εκτιμήσει ο οργανισμός την αξία των πληροφοριών. Η πολιτική πρέπει να εφαρμόζεται και για τις πληροφορίες που είναι αποθηκευμένες στους υπολογιστές και για τις πληροφορίες που περνούν από ένα δίκτυο.

ΕΠΙΠΕΔΑ ΔΙΑΔΙΚΤΥΟΥ

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

1.1 ΕΠΙΠΕΔΟ ΦΥΣΙΚΗΣ ΠΡΟΣΒΑΣΗΣ

Στο επίπεδο αυτό ανήκουν τα δίκτυα FDDI, ETHERNET και TOKEN RING. Το FDDI είναι ένα υψηλής επίδοσης οπτικό τοπικό δίκτυο δακτυλίου με σκυτάλη, που λειτουργεί στα 100 Mbps, σε αποστάσεις μέχρι 200 χμ. Το πρότυπο IEEE 802.3 γνωστό ως ETHERNET είναι ένα δίκτυο εκπομπής τύπου αρτηρίας με κατανεμημένο έλεγχο, το οποίο λειτουργεί με ταχύτητες των 10 ή 100 Mbps. Οι υπολογιστές που είναι συνδεδεμένοι στο ETHERNET μπορούν να μεταδώσουν όποτε θελήσουν. Αν δύο ή περισσότερα πακέτα συγκρουστούν, κάθε υπολογιστής απλώς περιμένει κάποιο τυχαίο χρονικό διάστημα και ξαναπροσπαθεί αργότερα. Το δίκτυο TOKEN RING είναι ένα τοπικό δίκτυο σε σχήμα δακτυλίου. Αυτή η αρχιτεκτονική επιτρέπει μόνο σε δύο σταθμούς εργασίας να ανταλλάξουν ταυτόχρονα δεδομένα. Αν ένας τρίτος σταθμός προσπαθήσει να μπει στο δίκτυο κατά την διάρκεια μιας ανταλλαγής δεδομένων, γίνεται σύγκρουση. Μετά από ελάχιστο χρονικό διάστημα (λίγα χιλιοστά του δευτερολέπτου), θα προσπαθήσει εκ νέου να μπει στο δίκτυο.

1.2 ΕΠΙΠΕΔΟ ΔΙΚΤΥΟΥ (IP ΠΡΩΤΟΚΟΛΛΟ)

Η μετάδοση στο *IP (Internet Protocol)* γίνεται με την τεχνική των *datagrams*. Το κάθε datagram (πακέτο) φθάνει στον παραλήπτη διασχίζοντας ένα η περισσότερα διασυνδεόμενα IP δίκτυα, χωρίς να εξαρτάται από άλλα προηγούμενα ή επόμενα πακέτα.

Το IP, σαν πρωτόκολλο του τρίτου επιπέδου, δεν ασχολείται με τις φυσικές συνδέσεις ή τον έλεγχο των ενδιάμεσων ζεύξεων μεταξύ των κόμβων του δικτύου. Αυτά είναι αρμοδιότητα των χαμηλότερων επιπέδων. Στην ουσία ασχολείται με την διευθυνσιοδότητη, τον τεμαχισμό και την επανασυγκόληση των πακέτων. Το πρωτόκολλο IP δεν είναι αξιόπιστης μεταφοράς *(reliable transfer)* καθώς δεν εξασφαλίζει την σίγουρη παράδοση των πακέτων με τεχνικές επανεκπομπής και έλεγχο ροής. Επιπλέον είναι *connectionless* γιατί δεν απαιτεί την αποκατάσταση σύνδεσης μεταξύ των δύο σημείων πριν την ανταλλαγή δεδομένων. Τα IP πακέτα μπορεί να ακολουθήσουν διαφορετικές διαδρομές και να φθάσουν με λανθασμένη σειρά στον αποδέκτη. Προβλήματα σαν αυτό αναλαμβάνουν να διορθώσουν το πρωτόκολλο TCP του ανωτέρου επιπέδου.

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

Δρομολόγηση

Τα IP πακέτα διασχίζουν το Διαδίκτυο από δρομολογητή σε δρομολογητή με κατεύθυνση τον τελικό αποδέκτη. Κάθε δρομολογητής διατηρεί πίνακες δρομολόγησης βάσει των οποίων το κάθε πακέτο αποστέλλεται στον επόμενο δρομολογητή που θα αναλάβει να το προωθήσει προς τον αποδέκτη του. Ο καθορισμός του επόμενου δρομολογητή γίνεται με την ανάγνωση της IP διευθύνσεως του παραλήπτη. Ανάλογα με το δίκτυο στο οποίο βρίσκεται ο παραλήπτης, επιλέγεται από τον πίνακα δρομολόγησης διαδεχόμενος router.

Όταν ένα πακέτο φθάσει σε ένα δρομολογητή αποθηκεύεται προσωρινά σε μία ουρά *(queue)*. Τα IP πακέτα επεξεργάζονται με την σειρά άφιξης τους. Κατά την επεξεργασίας τους, διαβάζεται η διεύθυνση του τελικού παραλήπτη. Εάν υπάρχει μποτιλιάρισμα στο δίκτυο, τότε η ουρά των πακέτων μέσα στον δρομολογητή μπορεί να γίνει μεγάλη, αυξάνοντας έτσι τις καθυστερήσεις μετάδοσης. Σε περίπτωση που η ουρά γίνει τόσο μεγάλη που να ξεπερνά τις χωρητικές δυνατότητες του δρομολογητή, τα πακέτα απορρίπτονται και χάνονται.

Διευθυνσιοδότηση

Καθ' ότι το Διαδίκτυο είναι μια εικονική κατασκευή που εφαρμόζεται λογισμικά, οι σχεδιαστές του είναι ελεύθεροι να διαλέξουν σχήμα διευθυνσιοδότησης που να μην σχετίζεται με κανένα υπάρχον δικτυακό υλικό. Το IP λειτουργεί με βάσει ένα νέο σετ διευθύνσεων που είναι ανεξάρτητο από τις υποκείμενες δικτυακές διευθύνσεις των υπολογιστών. Οι νέες αυτές διευθύνσεις καλούνται *Internet Addresses* ή *IP διευθύνσεις*.

Οι IP διευθύνσεις είναι φτιαγμένες έτσι ώστε να διευκολύνουν την δρομολόγηση. Κάθε IP πακέτο περιέχει την διεύθυνση του αποστολέα και του παραλήπτη, κάθε μια από τις οποίες έχει μήκος 32 bits. Μια IP διεύθυνση αποτελείται από δύο μέρη: το *netid* και το *hostid*. Το netid προσδιορίζει το δίκτυο στο οποίο βρίσκεται ο υπολογιστής, ενώ το hostid προσδιορίζει τον υπολογιστή. Ανάλογα με το μήκος της διευθύνσεως που αφιερώνεται σε κάθε τμήμα αυτής, οι διευθύνσεις διακρίνονται σε τρεις κλάσεις δικτύων:

Κλάση Α: 8 bit διεύθυνση δικτύου / 24 bit διεύθυνση υπολογιστή

Κλάση Β: 16 bit διεύθυνση δικτύου / 16 bit διεύθυνση υπολογιστή

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

Κλάση Γ: 24 bit διεύθυνση δικτύου / 8 bit διεύθυνση υπολογιστή

Επειδή οι IP διευθύνσεις κωδικοποιούν ένα δίκτυο αλλά και έναν υπολογιστή σε αυτό το δίκτυο, δεν καθορίζουν έναν συγκεκριμένο υπολογιστή, αλλά μία σύνδεση σε ένα δίκτυο.

Στην πράξη η απομνημόνευση των 32 bits είναι εξαιρετικά δύσκολη. Γι' αυτό έχει επινοηθεί η αναπαράσταση της διεύθυνσης με την χρήση δεκαδικών αριθμών. Η διεύθυνση διαχωρίζεται με τελείες σε τέσσερα πεδία των οκτώ bit.και Κκάθε πεδίο μετατρέπεται στο ισοδύναμο δεκαδικό αριθμό.

~~, όπως φαίνεται στο παρακάτω παράδειγμα.~~

Internet Control Message Protocol (ICMP)

Ένα άλλο πρωτόκολλο αυτού του επιπέδου είναι το *Internet Control Message Protocol (ICMP)*. Το ICMP δρα βοηθητικά, παράγοντας και διαχειρίζοντας μηνύματα λάθους για το πακέτο πρωτοκόλλων TCP/IP. Επιτρέπει στους δρομολογητές να επιστρέφουν μηνύματα λάθους σε άλλους δρομολογητές ή υπολογιστές. Για παράδειγμα, εάν ζητηθεί η σύνδεση με υπολογιστή που δεν υπάρχει ή δεν είναι διαθέσιμος προς το παρών, το ICMP σε κάποιον router θα επιστρέψει στον αποστολέα του αρχικού μηνύματος ένα μήνυμα με περιεχόμενο *"host unreachable"*. Επιπλέον, το ICMP μπορεί να χρησιμοποιηθεί για την συλλογή πληροφοριών για ένα δίκτυο και για σκοπούς debugging. Περαιτέρω και πιο αναλυτικές λεπτομέρειες για το ICMP υπάρχουν στο RFC 792.

1.3 ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΩΝ

Σε αυτό το επίπεδο ανήκουν οι υπηρεσίες του Διαδικτύου. Θα περιγράψουμε τις σημαντικότερες και τις πιο συχνά χρησιμοποιούμενες.

Telnet

Το Telnet (ή *remote login*) είναι μια από τις βασικότερες υπηρεσίες του Διαδικτύου που επιτρέπει σε κάποιον χρήστη να έχει πρόσβαση τερματικού σε ένα μακρινό server. Το Telnet λειτουργεί μεταφέροντας τις εντολές που πληκτρολογεί ο χρήστης στον υπολογιστή του στον απομακρυσμένο υπολογιστή με τον οποίο συνδέεται. Παρ' όλο που στην πραγματικότητα ο χρήστης "μιλάει" με τον υπολογιστή του, το πρόγραμμα καταφέρνει και δίνει

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

την ψευδαίσθηση στον χρήστη ότι επικοινωνεί με τον απομακρυσμένο υπολογιστή.

File Transfer Protocol (FTP)

Το FTP ήταν η πρώτη υπηρεσία για την ανάκτηση και μεταφορά πληροφορίας και αρχείων που χρησιμοποιήθηκε στο Διαδίκτυο. Η βασική λειτουργία του είναι η αξιόπιστη μεταφορά αρχείων από υπολογιστή σε υπολογιστή και επιτρέπει στους χρήστες να στήνουν μια σύνδεση ελέγχου μεταξύ του FTP client και του FTP server. Η σύνδεση αυτή τους επιτρέπει να ψάχνουν στους καταλόγους του server και να μεταφέρουν τα αρχεία που επιθυμούν από τον server προς τον δικό τους υπολογιστή. Για την μεταφορά των αρχείων δημιουργείται αυτόματα από τοθ FTP μια νέα ανεξάρτητη σύνδεση.

Domain Name Service (DNS)

Η υπηρεσία DNS χρησιμοποιείται από τους χρήστες του Διαδικτύου για την αντικατάσταση των αριθμητικών IP διευθύνσεων με εύχρηστα ονόματα (domain names). Συγκεκριμένα, το DNS προσφέρει υπηρεσίες μετάφρασης μεταξύ ονομάτων και IP διευθύνσεων. Κάθε υπολογιστής και δρομολογητής στο Διαδίκτυο διαθέτει ένα όνομα. Η ονοματολογία του Διαδικτύου έχει σαν χαρακτηριστικό την ιεράρχηση των ονομάτων. Κατατάσσονται ανάλογα με το εύρος του δικτύου που περιγράφουν και το όνομα ενός μηχανήματος αποτελείται από τόσα επιμέρους ονόματα όσα χρειάζεται για να προσδιοριστεί πλήρως. Τα επιμέρους ονόματα δικτύων διαχωρίζονται μεταξύ τους με τελείες. Για παράδειγμα, το όνομα teleinfom.teiep.gr αντιπροσωπεύει τοvο τμήμα τηλεπληροφορικής ~~υπολογιστή με το όνομα *saturn* που βρίσκεται στο τοπικό δίκτυο *lab.epmhs.gr*~~που βρίσκεται με την σειρά του στο ευρύτερο δίκτυο teiep.gr, το οποίο ανήκει στην περιοχή gr, δηλαδή στην Ελλάδα.

Σε ένα δίκτυο που εξυπηρετεί αρκετούς υπολογιστές κάτω από το ίδιο όνομα δικτύου πρέπει να λειτουργεί ένας DNS server που θα παρέχει πληροφορίες για τους υπολογιστές που ανήκουν στο δίκτυο του. Για κάθε επίπεδο αυτής της ιεράρχησης υπάρχει τουλάχιστον ένας DNS server που γνωστοποιεί το όνομα του στον server του αμέσως ανώτερου επιπέδου. Αυτό επαναλαμβάνεται έως ότου να καλυφθεί όλη ιεραρχία ονομάτων.

Η υπηρεσία του DNS χρησιμοποιείται αυτοματοποιημένα και από τις υπόλοιπες εφαρμογές του Διαδικτύου. Όποτε απευθύνεται στον DNS server

Formatted: Line spacing: 1,5 lines

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

ερώτημα για κάποιον υπολογιστή από οποιαδήποτε υπηρεσία, αυτός συμβουλεύεται τους πίνακες καταχωρήσεων που διαθέτει και δίνει απάντηση για την IP διεύθυνση που αντιστοιχεί στο όνομα του ζητούμενου υπολογιστή. Σε περίπτωση που ερωτηθεί για υπολογιστή για τον οποίο δεν έχει καταχώρηση, τότε παραπέμπει την αίτηση σε DNS server υψηλότερου επιπέδου.

Ηλεκτρονικό Ταχυδρομείο (E-mail)

Το ηλεκτρονικό ταχυδρομείο επιτρέπει την αποστολή μηνυμάτων μεταξύ των χρηστών του Διαδικτύου. Οι διευθύνσεις του ηλεκτρονικού ταχυδρομείου βασίζονται στις διευθύνσεις του Internet και έχουν την μορφή *"user@domain"*, όπου *user* το όνομα του χρήστη και *domain* το όνομα του υπολογιστή. Παρακάτω φαίνεται πως μεταφέρονται τα ηλεκτρονικά μηνύματα. *Ο User Agent (UA)* είναι το πρόγραμμα client στον υπολογιστή του χρήστη που αναλαμβάνει την διαχείριση και ανάκτηση του ταχυδρομείου. Με την βοήθεια αυτού του προγράμματος ο χρήστης γράφει τα μηνύματα του, τα στέλνει, παραλαμβάνει άλλα μηνύματα και τα διαβάζει. Ο *Mail Transfer Agent (MTA)* παραλαμβάνει τα μηνύματα από τον UA και τα προωθεί στον επόμενο MTA μέχρι να βρεθεί ο MTA που έχει άμεση σύνδεση με τον υπολογιστή του χρήστη. Ο τελευταίος MTA επικοινωνεί με τον UA του παραλήπτη για την παράδοση των μηνυμάτων. Το σύνολο των MTA καλείται *Message Transfer System (MTS)*.

Η επικοινωνία από MTA σε MTA γίνεται με χρήση του πρωτοκόλλου *SMTP (Simple Mail Transfer Protocol*, ενώ η επικοινωνία του UA με τον MTA γίνεται με χρήση των πρωτοκόλλων *POP (Post Office Protocol)* και IMAP *(Internet Message Access Protocol)*. Τα ίδια τα μηνύματα συντάσσονται με ~~βάσει~~ βάση το πρωτόκολλο *MIME (Multipurpose Internet Mail Extensions)* ή με το RFC822.

Το παραπάνω σύστημα παράδοσης του ηλεκτρονικού ταχυδρομείου επιτρέπει το ηλεκτρονικό ταχυδρομικό του χρήστη να βρίσκεται σε κάποιον server και έτσι δεν είναι απαραίτητο να είναι εν λειτουργία ο υπολογιστής του αποδέκτη κατά την αποστολή του μηνύματος. Ο αποδέκτης θα παραλάβει τα μηνύματα του όταν ανοίξει τον υπολογιστή του και συνδεθεί με τον server (MTA).

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

World Wide Web (WWW)

Είναι από τις τελευταίες και πιο γρήγορα αναπτυσσόμενες υπηρεσίες του Διαδικτύου. Το *World Wide Web (WWW)* επιτρέπει την πρόσβαση και την ανάκτηση κάθε είδους πληροφορίας, μέσα από ένα σύνθετο περιβάλλον γραφικών, κειμένου και φωτογραφιών. Το WWW αποτελείται από υπολογιστές που διανείμουν την πληροφορία, τους servers και από υπολογιστές που αναζητούν πληροφορίες εκ μέρους των χρηστών, τους clients. Οι πρώτοι τρέχουν ειδικά προγράμματα που καλούνται *Web servers*, ενώ οι δεύτεροι τρέχουν τους *Web browsers*, client προγράμματα που διατίθονται δωρεάν από πολλές εταιρίες.

Η πληροφορία αποθηκεύεται στους Web servers (συνήθως ένας αφιερωμένος υπολογιστής ταυτίζεται με το λογισμικό που τρέχει) υπό μορφή ηλεκτρονικών σελίδων. Η γλώσσα που χρησιμοποιείται για την σύνταξη των σελίδων αυτών είναι η *HTML (Hyper Text Mail Language)*. Τα περιεχόμενα της μπορεί να είναι δεδομένα κειμένου, γραφικά, εικόνες, σύνδεσμοι και τώρα τελευταία με την ανάπτυξη της Java, αλληλεπιδραστικές διεργασίες *(interactive sessions)*. Επίσης, με την χρήση του πρωτοκόλλου MIME που αναφέραμε παραπάνω, μπορεί να προστεθεί στις σελίδες κινούμενη εικόνα, ήχος και κινούμενα γραφικά.

Η θέση μιας σελίδας στο Διαδίκτυο καθώς και το πρωτόκολλο που χρειάζεται για να την ανοίξει κάποιος προσδιορίζεται από το λεγόμενο *URL (Uniform Resource Locator)*. Το URL προσδιορίζει επιπλέον το όνομα του αρχείου και του καταλόγου στον Web server. Τα πρωτόκολλα που χρησιμοποιούνται για το άνοιγμα των ηλεκτρονικών σελίδων και γενικότερα για την επικοινωνία μεταξύ του Web server και του Web browser, είναι κυρίως το *HTTP (Hyper Text Transfer Protocol)*. Άλλα πρωτόκολλα που μπορούν να χρησιμοποιηθούν είναι το *FTP* και το *GOPHER*.

Η μορφή του URL είναι:

<protocol>://<hostname>:<port><directory><filename>

όπου <protocol> είναι το χρησιμοποιούμενο πρωτόκολλο, <hostname> το όνομα του Web server, <port> η χρησιμοποιούμενη πόρτα επικοινωνίας (συχνά παραλείπεται και χρησιμοποιείται η προκαθορισμένη τιμή που είναι 80), <directory> ο κατάλογος στον Web server που περιέχει το ζητούμενο αρχείο και τέλος <filename> το όνομα του αρχείου – ηλεκτρονική σελίδα που

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

ζητήθηκε.

Τα περιεχόμενα της ηλεκτρονικής σελίδας μπορεί να είναι στατικά ή να δημιουργούνται δυναμικά με την εκτέλεση ενός προγράμματος στην μεριά τους server. Ένα τυποποιημένο μέσο για την γραφή τέτοιων προγραμμάτων είναι το *CGI (Common Gateway Interface)*.

ΚΕΦΑΛΑΙΟ 2

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ

2.1 Λόγοι Ανασφάλειας

Υπάρχουν συγκεκριμένοι λόγοι που το Διαδίκτυο είναι ανασφαλές σε σχέση με άλλα κλειστά δίκτυα:

- Τα στάνταρ που χρησιμοποιούνται για τα βασικά πρωτόκολλά του διαδικτύου είναι δημόσια. Αυτό σημαίνει ότι κακόβουλοι χρήστες έχουν πολλές πληροφορίες για τον τρόπο λειτουργίας του διαδικτύου. Επίσης, η ανοιχτή φύση του διαδικτύου υπονομεύει την ασφάλεια, αφού όλες οι επιθέσεις και οι αδυναμίες γίνονται αμέσως γνωστές και τα προγράμματα που τα αντιμετωπίζουν εκδίδονται αμέσως.
- Το διαδίκτυο είναι διαδεδομένο. Βρίσκεται σε σπίτια, σε καφετέριες, σε βιβλιοθήκες και σε γραφεία. Δεν απαιτείται πολύπλοκο υλικό για κάποια μη εξουσιοδοτημένη πρόσβαση: ένας προσωπικός υπολογιστής και ένας φυλλομετρητής διαδικτύου θα σας επιτρέψουν την γρήγορη πρόσβαση στην ιστοσελίδα ενός οικονομικού οργανισμού.
- Οι διακομιστές διαδικτύου είναι επεκτάσιμοι: μπορούν να συνδεθούν σε πολλές τεχνολογίες, για παράδειγμα συστήματα διαχείρισης δεδομένων. Το λογισμικό που διαχειρίζεται αυτές τις επεκτάσεις είναι αρκετά πολύπλοκο και μπορεί να μετατρέψει ένα διακομιστή διαδικτύου σε κάτι που δεν είχε σκοπό να γίνει. Ένα τέτοιο λογισμικό είναι ευπαθές σε επιθέσεις.
- Η ταχύτατη ανάπτυξη του διαδικτύου είχε σαν αποτέλεσμα το σχετικό λογισμικό να αναπτυχθεί χωρίς να δοθεί μεγάλη προσοχή σε θέματα ασφαλείας. Τα πιο ασφαλή συστήματα είναι αυτά που σχεδιάστηκαν λαμβάνοντας υπόψιν τους εξ αρχής την ασφάλεια.

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

- Το διαδίκτυο περιέχει πολλά αλληλοσυνδεδεμένα στοιχεία που απαιτούν το ένα το άλλο για να εκτελέσουν βασικές λειτουργίες.
- Οι φυλλομετρητές διαδικτύου είχαν στην αρχή περιορισμένη λειτουργικότητα. Στην αρχή δεν ήταν τίποτα παραπάνω από προγράμματα που απλώς κατέβαζαν αρχεία κειμένου από τους διακομιστές διαδικτύου.
- Η ταχύτητα ανάπτυξης του διαδικτύου απαιτούσε και τη συνεχή βελτίωση, ώστε να ανταποκριθούν στις αυξανόμενες απαιτήσεις λειτουργικότητας. Αυτό γινόταν δυνατόν μέσω ανασφαλών προσθετικών προγραμμάτων (**plug-ins)**, που είχαν σοβαρά προβλήματα ασφαλείας.

  Ένας μύθος για την ασφάλεια υπολογιστών.

  Ένας μύθος για την ασφάλεια υπολογιστών είναι ότι οι διάφορες επιθέσεις γίνονται από ειδικούς σε θέματα λογισμικού με τεράστιες ικανότητες σε τεχνολογικά θέματα. Ενώ αυτό είναι μερικώς σωστό, υπάρχουν πολλά δικτυακά εγκλήματα που απαιτούν λίγα προσόντα. Για παράδειγμα, σ' ένα περιβάλλον με λίγους φυσικούς ελέγχους, μπορεί να είναι εύκολη η ανακάλυψη κωδικών. Την επόμενη φορά που θα επισκεφτείτε μια εταιρία προσέξτε ορισμένους πίνακες ανακοινώσεων - θα δείτε περιστασιακά κάποια λέξη γραμμένη στη γωνία για να θυμίζει στο χρήστη του γραφείου τους κωδικούς.

Μια άλλη πλευρά της ασφάλειας στο διαδίκτυο είναι ότι αφού η επικοινωνία είναι τόσο γρήγορη και μπορεί να αυτοματοποιηθεί, σημαίνει ότι και οι εγκληματίες μπορούν να αυτοματοποιήσουν διαδικασίες που παλιότερα θα τις υλοποιούσαν σε μεγάλο χρονικό διάστημα. Το διαδίκτυο ξαναέδωσε ζωή σε απάτες που είχαν σχεδόν εξαλειφθεί. Ένα παράδειγμα είναι η απάτη Ponzi, που ονομάστηκε από τον απατεώνα του προηγούμενου αιώνα Charles Ponzi. Αυτή υπόσχεται σε επενδυτές ένα τεράστιο επιτόκιο σαν αποτέλεσμα μιας απάτης όπως η καλλιέργεια ενός άγνώστου σπόρου σε μια τριτοκοσμική χώρα. Ο απατεώνας παίρνει τα χρήματα που του εμπιστεύτηκαν και αρχικά πληρώνει στους επενδυτές τις προβλεπόμενες αποδόσεις. Αυτοί οι επενδυτές χρησιμοποιούνται για να φέρουν άλλους επενδυτές. Τελικά ο απατεώνας εξαφανίζεται με τα περισσότερα κεφάλαια. Αφού οι λίστες ηλεκτρονικών διευθύνσεων βρίσκονται πολύ εύκολα και υπάρχουν προγράμματα για μαζική αποστολή ηλεκτρονικών μηνυμάτων, τα τελευταία χρόνια ξαναεμφανίστηκαν οι απάτες με βάση τις πυραμίδες.

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

2.2 Τύποι επιθέσεων

Αυτή η ενότητα εξετάζει μερικούς από τους τρόπους με τους οποίους διαπράττονται παράνομες δραστηριότητες στο Internet. Αυτές κυμαίνονται από ενέργειες οι οποίες απλά εκμεταλλεύονται την απλή ανθρώπινη αδυναμία έως αυτές που απαιτούν εξειδικευμένες τεχνολογικές γνώσεις και βαθιά κατανόηση της δομής του Internet. Ωστόσο, πριν εξετάσουμε αυτούς τους τρόπους με τους οποίους μπορεί να απειληθεί ένα σύστημα, αξίζει να δούμε τους τύπους απειλών που μπορεί να αντιμετωπίσει ένα Web site. Ο Stallings τις κατέταξε ως εξής:

- *Απειλές ακεραιότητας δεδομένων*. Αυτές οι απειλές αφορούν την παραποίηση αποθηκευμένων δεδομένων από έναν εισβολέα όπως την αλλαγή στοιχείων πιστωτικών καρτών σε μια βάση δεδομένων ή την παραποίηση στοιχείων κατά την μεταφορά τους όπως την μεταβολή ενός μηνύματος κατά τη μεταφορά του.
- *Απειλές εμπιστευτικών δεδομένων*. Αυτές οι απειλές αφορούν την ανάγνωση σημαντικών αποθηκευμένων δεδομένων από μη εξουσιοδοτημένα άτομα όπως π.χ. διοικητικά μυστικά εταιρειών κ.λ.π.
- *Απειλές άρνησης υπηρεσιών (Denial of Service - DoS).* Αυτές οι απειλές αφορούν το πλημμύρισμα ενός Web server με μεγάλο αριθμών αιτημάτων ώστε να μην μπορεί πλέον αυτός να λειτουργήσει λόγω έλλειψης πόρων.
- *Απειλές πιστοποίησης χρηστών.* Σε τέτοιου είδους απειλές ο εισβολέας προσποιείται πως είναι ένας χρήστης ενώ δεν είναι, για παράδειγμα κάποιος ο οποίος έχει κάποιο συγκεκριμένο τραπεζικό λογαριασμό.

2.3 Αυτά οδηγούν σε μια σειρά απαιτήσεων για ~~ασφαλείς~~ Ασφαλείς Εεφαρμογές Ηηλεκτρονικού Εεμπορίου:

- *Εμπιστευτικότητα*. Αυτό σημαίνει πως πληροφορίες οι οποίες αποθηκεύονται σε κάποιο σύστημα δεν μπορούν να είναι προσβάσιμες από μη εξουσιοδοτημένους χρήστες.
- *Πιστοποίηση*. Αυτό σημαίνει πως η πηγή ενός μηνύματος ή συναλλαγής προσδιορίζεται σωστά και ότι η πηγή του μηνύματος ή της

Formatted: Line spacing: 1,5 lines
Formatted: Font: 14 pt
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: 14 pt
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

συναλλαγής είναι αυτός που λέει πως είναι. Για παράδειγμα, κάποιος ο οποίος μπορεί να χρησιμοποιήσει μια δικτυακή υπηρεσία και πλήρωσε για αυτή πρέπει να αναγνωρίζεται με σωστό τρόπο από το σύστημα.

- *Ακεραιότητα*. Αυτό σημαίνει ότι μόνο εξουσιοδοτημένη χρήστες μπορούν να αλλάξουν τα δεδομένα που χρησιμοποιεί ένα σύστημα.
- *Μη άρνηση αναγνώρισης ανταλλαγής μηνύματος*. Αυτό σημαίνει πως ούτε ο αποστολέας είτε ο παραλήπτης κάποιου μηνύματος θα μπορεί να αρνηθεί ότι έγινε η ανταλλαγή κάποιου μηνύματος.
- *Έλεγχος πρόσβασης*. Αυτό σημαίνει πως οι υπηρεσίες σε ένα σύστημα ηλεκτρονικού εμπορίου ελέγχονται ώστε οι χρήστες επιτρέπεται μόνο να χρησιμοποιήσουν τους πόρους που χρειάζονται και είναι εξουσιοδοτημένοι να χρησιμοποιήσουν.
- *Διαθεσιμότητα συστήματος*. Αυτό σημαίνει ότι οι υπηρεσίες του συστήματος είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες όποτε αυτές χρειάζονται.

ΚΕΦΑΛΑΙΟ 3

ΕΡΓΑΛΕΙΑ ΑΣΦΑΛΕΙΑΣ

Κρυπτογραφία και εργαλεία κρυπτογραφίας

Σε αυτή την ενότητα περιγράφεται η κυριότερη τεχνολογία ασφαλείας, η κρυπτογραφία, καθώς επίσης και κάποια σχετικά εργαλεία και τεχνικές.

3.1 Τα βασικά της κρυπτογραφίας

Η προηγούμενη ενότητα εξέτασε διάφορα είδη απειλών που μπορεί να αντιμετωπίσει ένας υπολογιστής συνδεδεμένος σε ένα δίκτυο. Αυτή η ενότητα εξετάζει την κύρια τεχνολογία, η οποία έδωσε πολλά εργαλεία που βελτιώνουν την άμυνα ενός συστήματος από τους πιθανούς εισβολείς. Η τεχνολογία αυτή είναι η **κρυπτογραφία**.

Ο όρος 'κρυπτογραφία' αναφέρεται σε ένα σύνολο τεχνικών που χρησιμοποιούνται για να διασφαλίσουν ότι τα δεδομένα δεν μπορούν να διαβαστούν από κάποιον που δεν είναι ο αποστολέας ή κανονικός παραλήπτης τους. Περιλαμβάνει την μετατροπή ενός συνόλου δεδομένων (το αποκαλούμενο **απλό κείμενο δεδομένων)** σε μια μπερδεμένη και δυσνόητη

Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

μορφή (αποκαλούμενη **κρυπτογραφημένο κείμενο δεδομένων**). Για παράδειγμα, θα μπορούσε να γίνεται απλά με το ανακάτεμα των γραμμάτων ενός μηνύματος με προκαθορισμένο τρόπο, π.χ. του 'I am here' σε 'heIm a er' - αυτό βέβαια είναι πάρα πολύ απλό και αποτελεί ένα κώδικα που μπορεί να σπάσει εύκολα.

ROT13

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Μια πάρα πολύ απλή μέθοδος κρυπτογράφησης είναι η ROT13. Η μέθοδος συνίσταται απλά στην αντικατάσταση κάθε χαρακτήρα που εμφανίζεται στο μήνυμα με τον χαρακτήρα που προκύπτει αν πάμε 13 θέσεις μπροστά στο αλφάβητο, π.χ. αντικαθιστούμε το Α με το Ν. Αυτή η μέθοδος είναι πάρα πολύ ευάλωτη, δεν προσφέρει κάποια σημαντική προστασία και μπορεί να δείτε κάποια παραλλαγή της σε newsgroups και forums.

Οι πρώτες μέθοδοι κρυπτογράφησης χρησιμοποιούσαν δυο τρόπους αλλαγής του αρχικού μηνύματος: την **αντικατάσταση** και τον **μετασχηματισμό**. Ο πρώτος γίνεται αντικαθιστώντας διακριτά κομμάτια του αρχικού κειμένου με άλλα, π.χ. αλλάζοντας κάθε δυάδα γραμμάτων με κάποια άλλα βάσει ενός προκαθορισμένου κώδικα ενώ ο άλλος γίνεται με σύνθετους μετασχηματισμούς μεταξύ πολλών κομματιών του αρχικού κειμένου. Κατά τη διάρκεια του εικοστού αιώνα κατασκευάστηκαν αρκετές μηχανικές συσκευές που έκαναν αυτόματα αντικατάσταση, πιο διάσημη από τις οποίες ήταν πιθανότατα η συσκευή Enigma που χρησιμοποιήθηκε από τους Γερμανούς κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου για την αποστολή μυστικών μηνυμάτων στα στρατεύματα τους. Ο κώδικας του έσπασε από τους συμμάχους, ωστόσο οι Γερμανοί δεν ήξεραν ότι τα μυστικά τους αποκρυπτογραφούνταν και αυτό συντέλεσε σύμφωνα με τους ιστορικούς στην τελική τους ήττα. Οι μέθοδοι που χρησιμοποιούνται από την σύγχρονη κρυπτογραφία βασίζονται και στην αντικατάσταση και τον μετασχηματισμό.

Η μοντέρνα κρυπτογραφία βασίζεται σε εξαιρετικά πολύπλοκους, επαληθευμένους για την ορθότητα τους αλγορίθμους για την μετατροπή ενός απλού κειμένου σε κρυπτογραφημένο, με την διαδικασία να είναι γνωστή ως **κρυπτογράφηση**. Οι αλγόριθμοι που χρησιμοποιούνται αλλάζουν τη λειτουργία τους βάσει ενός **κλειδιού**. Αυτό είναι ένα σύνολο χαρακτήρων που αλλάζουν τον τρόπο με τον οποίο γίνεται η μετατροπή του αρχικού κειμένου. Ένα πολύ απλό παράδειγμα είναι ένας αλγόριθμος ο οποίος θα

Formatted: Right: 0,63 cm

αντικαταστήσει κάθε χαρακτήρα σε ένα κείμενο με τον ASCII χαρακτήρα που βρίσκεται *n* θέσεις μπροστά στον πίνακα των ASCII κωδικών, με το κλειδί να είναι το *n*. Φυσικά αυτός είναι ένας πολύ απλός και ευάλωτος αλγόριθμος.

Όταν το κωδικοποιημένο κείμενο παραληφθεί, ο παραλήπτης χρησιμοποιεί τον αλγόριθμο και το κλειδί για να ανακτήσει το αρχικό μήνυμα. Αυτή είναι μια διαδικασία γνωστή ως **αποκρυπτογράφηση**.

Τα τελευταία 20 χρόνια υπήρξε πολύ μεγάλη πρόοδος στον τομέα της κρυπτογραφίας. Πριν τη δεκαετία του 1970 η κρυπτογραφία σχετιζόταν κυρίως με στρατιωτικές εφαρμογές, ωστόσο η άφιξη των δικτυακών τεχνολογιών έκανε την κρυπτογραφία να χρησιμοποιείται πλέον περισσότερο σε μη στρατιωτικές εφαρμογές.

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

3.2 Κρυπτογραφία συμμετρικού κλειδιού

Formatted: Font: (Default) Arial

Χρησιμοποιούνται κυρίως δυο μορφές κρυπτογραφίας σε δίκτυα υπολογιστών: η **κρυπτογραφία συμμετρικού κλειδιού** και η **κρυπτογραφία δημοσίου κλειδιού**. Η πρώτη περιγράφηκε ήδη και περιλαμβάνει ένα αριθμό βημάτων:

- Ο αποστολέας ενός μηνύματος κρυπτογραφεί το μήνυμα χρησιμοποιώντας έναν αλγόριθμο που βασίζεται σε κλειδί.
- Το κρυπτογραφημένο μήνυμα στέλνεται μέσω του (ανασφαλούς) δικτύου, π.χ. μέσω του Internet.
- Το κλειδί μεταφέρεται με κάποιο ασφαλή τρόπο στον παραλήπτη.
- Ο παραλήπτης λαμβάνει το κλειδί και το χρησιμοποιεί για να αποκρυπτογραφήσει το μήνυμα που έλαβε.

Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ αποδοτική όσον αφορά τους πόρους που απαιτούνται, ωστόσο έχει ένα βασικό πρόβλημα: ότι πρέπει το κλειδί να μεταφερθεί μέσω ενός ασφαλούς μέσου και πιθανόν θα μπορούσε η μετάδοση του να θέσει σε κίνδυνο την ασφάλεια του κρυπτογραφημένου μηνύματος. Περαιτέρω, δεν κάνει διάκριση μεταξύ αποστολέα και παραλήπτη. Υπάρχουν ωστόσο κάποιοι αλγόριθμοι

Formatted: Right: 0,63 cm

συμμετρικού κλειδιού που ακόμη χρησιμοποιούνται:

- *DES*. Αυτός ο αλγόριθμος έχει τυποποιηθεί από την αμερικάνικη κυβέρνηση και χρησιμοποιείται από το 1977. Ο DES μετασχηματίζει μπλοκ χαρακτήρων αντί για απλούς χαρακτήρες. Χρησιμοποιεί κλειδί μεγέθους 56 bit και μπορεί να λειτουργήσει με διάφορους τρόπους ανάλογα με το επίπεδο ασφαλείας που απαιτείται. Ο DES είναι ένας αρκετά ισχυρός αλγόριθμος κρυπτογράφησης, ωστόσο κάποιοι εμπειρογνώμονες ασφαλείας λένε πως μπορεί να σπάσει από έναν υπολογιστή ειδικού σκοπού σχεδιασμένο για το σπάσιμο κωδικών. Η πιστοποίηση του DES ανακλήθηκε το 1998 και αντικαταστάθηκε από έναν άλλο αλγόριθμο γνωστό ως 3DEA.

  Το σπάσιμο του DES

  Ένας διαγωνισμός που εμφανίζεται τακτικά στο Internet αφορά το σπάσιμο ενός κρυπτογραφημένου μηνύματος σε χρόνο ρεκόρ. Το 1999 μια ομάδα ερευνητών και χρηστών υπολογιστών αποκρυπτογράφησε ένα μήνυμα κωδικοποιημένο σε τον DES σε 22 ώρες χρησιμοποιώντας 100000 υπολογιστές σε όλο τον κόσμο. Η υπολογιστική εργασία που χρειάστηκε για να σπάσει ο κώδικας κατανεμήθηκε σε όλους αυτούς τους υπολογιστές και συντονίστηκε από κάποιους άλλους υπολογιστές. Αυτή η μορφή μαζικής κατανεμημένης επεξεργασίας διαδίδεται όλο και περισσότερο στο Internet. Για παράδειγμα, υπάρχει ένα σύστημα το οποίο χρησιμοποιεί τον αδρανή χρόνο υπολογιστών σε όλο τον κόσμο για να αναλύσει ραδιοκύματα από το διάστημα και να εντοπίσει τυχόν σήματα που παρουσιάζουν δομή και προέρχονται από εξωγήινους ενώ υπάρχει και ένα άλλο σύστημα για τον υπολογισμό του π με ένα πολύ μεγάλο αριθμό δεκαδικών ψηφίων
- *Τριπλό DES*. Όπως είναι προφανές και από το όνομα του, αυτός είναι ο αλγόριθμος είναι μια παραλλαγή του DES. Γίνεται με την επανάληψη τρεις φορές του DES σε απλό κείμενο. Ο αλγόριθμος αυτός χρησιμοποιήθηκε από οικονομικούς οργανισμούς όπως τράπεζες σαν μια πιο ασφαλής λύση από τον DES.
- *Blowfish*. Αυτός είναι ένας αλγόριθμος που χρησιμοποιεί κλειδί μήκους 448 bit. Δεν υπάρχει πατέντα για αυτό τον αλγόριθμο και μπορεί να χρησιμοποιηθεί από οποιονδήποτε.
- *IDEA*. Αυτός είναι ένας αλγόριθμος που αναπτύχθηκε στην Ελβετία και

Formatted: Right: 0,63 cm

δημοσιοποιήθηκε το 1990. Χρησιμοποιεί ένα κλειδί μεγέθους 128 bit και δεν είναι πατενταρισμένος.

- *RC2*. Αυτός είναι ένας αλγόριθμος που αναπτύχθηκε από τον αμερικανό ερευνητή συστημάτων ασφαλείας Ronald Rivest. Μετασχηματίζει μπλοκ δεδομένων και χρησιμοποιεί ένα κλειδί μεγέθους από 1 εως 128 bits.
- *RC4*. Αυτός είναι ένας αλγόριθμος που μετασχηματίζει το αρχικό κείμενο χαρακτήρα - χαρακτήρα. Αρχικά ήταν ένα εμπορικό μυστικό αλλά αργότερα δημοσιεύτηκε το σε ένα newsgroup το 1994. Μπορεί να χρησιμοποιήσει ένα κλειδί μεγέθους μεταξύ 1 και 2048 bits. Και αυτός ο αλγόριθμος, όπως ο RC2, αναπτύχθηκε από τον Ronald Rivest.
- *RC5*. Αυτός είναι άλλος ένας αλγόριθμος του Ronald Rivest και αναπτύχθηκε το 1994.

3.3 Επιθέσεις σε αλγορίθμους συμμετρικού κλειδιού

Formatted: Font: (Default) Arial

Υπάρχουν διάφοροι τρόποι με τους οποίους ένας αλγόριθμος συμμετρικού κλειδιού μπορεί να δεχθεί επίθεση. Ο πιο απλός είναι η δοκιμή όλως των δυνατών κλειδιών μέχρι να προκύψει κάποιο κείμενο που φαίνεται να έχει λογικό περιεχόμενο. Αυτό μπορεί να φαίνεται μια όχι και τόσο έυκολη δυνατότητα αλλά αν το μέγεθος του κλειδιού είναι σχετικά μικρό, τότε είναι εφικτό. Ωστόσο όταν χρησιμοποιούνται μεγάλα κλειδιά, για παράδειγμα με 128 bits, αυτή η μέθοδος γίνεται ανέφικτη.

Σπάσιμο κωδικών με κλειδί 40 bit και το "κόστος δυνατότητας σπασίματος"

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Το 1994 ήταν δυνατό να φτιαχτεί ένας υπολογιστής αξίας 20000 δολαρίων που θα μπορούσε να εξετάζει 150000 κλειδιά σε ένα δευτερόλεπτο και το 1997 ένας κώδικας των 40 bit αποκωδικοποιήθηκε μόνο σε 3.5 ώρες. Η ισχύς των υπολογιστών αυξήθηκε σημαντικά από τότε ώστε πλέον μπορούν να σπάσουν και κώδικες με μεγαλύτερα κλειδιά. Αυτό οδήγησε του ερευνητές που εργάζονται στον τομέα της κρυπτογραφίας να δημιουργήσουν τον όρο "κόστος δυνατότητας σπασίματος". Αυτό είναι ο αριθμός των bits που πρέπει να προστεθούν σε ένα κλειδί ενός κρυπτογραφικού αλγορίθμου ώστε να τον κρατήσουν ασφαλή σε σχέση με την τρέχουσα ποσότητα υπολογιστικής ισχύος.

Υπάρχουν ωστόσο και καλύτεροι τρόποι σπασίματος ενός αλγορίθμου

Formatted: Right: 0,63 cm

συμμετρικού κλειδιού. Ένας απλός είναι να κλέψετε το κλειδί. Υπάρχουν και άλλες που περιγράφονται παρακάτω..

Η πρώτη είναι μια μορφή επίθεσης γνωστή ως **επίθεση γνωστού κειμένου.** Αυτή η τεχνική βασίζεται στο γεγονός ότι ο υποκλοπέας έχει ένα παράδειγμα απλού κειμένου μαζί με το αντίστοιχο του κωδικοποιημένο μήνυμα. Από αυτά ο υποκλοπέας μπορεί να υπολογίσει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση και στη συνέχεια μπορεί να το χρησιμοποιήσει για να αποκωδικοποιήσει εύκολα και άλλα μηνύματα. Η απόκτηση ενός δείγματος κρυπτογραφημένου κειμένου και του αντίστοιχου αρχικού κειμένου είναι αρκετές φορές ~~αρκετά~~ πολύ εύκολη ~~αφού αρκετές φορές~~ συχνα ένα μέρος των μηνυμάτων που ανταλλάσσονται είναι αρκετά απλό να βρεθεί, για παράδειγμα ~~τα~~ όταν έχουν κάποια σταθερή μορφή επικεφαλίδας κ.λ.π.

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Το δεύτερο είδος επίθεσης είναι η **επίθεση επιλεγμένου κειμένου**. Σε αυτό το είδος επίθεσης ζητά από τον υπολογιστή που εκτελεί την αποκρυπτογράφηση να κωδικοποιήσει ένα ειδικό κομμάτι κειμένου, το οποίο έχει επιλεγεί ώστε η γνώση του αντίστοιχου κρυπτογραφημένου κειμένου να παρέχει αρκετά στοιχεία για το κλειδί.

Το τρίτο είδος επίθεσης είναι γνωστή ως **διαφορική επίθεση κρυπτανάλυσης**. Εδώ ο υποκλοπέας δημιουργεί μια σειρά μηνυμάτων που διαφέρουν ελάχιστα μεταξύ τους και εξετάζει πάλι την αντίστοιχη κρυπτογραφημένη έκδοση τους. Με τον τρόπο αυτό ο υποκλοπέας μπορεί να αποκτήσει σημαντικές πληροφορίες για το κλειδί.

Η τελευταία μορφή επίθεσης είναι γνωστή ως **διαφορική επίθεση λαθών**. Αυτή είναι μια επίθεση με hardware όπου η συσκευή κωδικοποίησης δέχεται πίεση συγκεκριμένης μορφής ώστε να κάνει λάθη. Με προσεκτική εξέταση των λαθών αυτών μπορεί να ανιχνευθεί το κλειδί.

3.4 Κρυπτογραφία δημοσίου κλειδιού

Formatted: Font: (Default) Arial, 14 pt

3.4.1 Η ιδέα

Formatted: Font: (Default) Arial

Αυτή είναι μια μορφή κρυπτογραφίας που δεν απαιτεί τη χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος αλλά χρησιμοποιεί δυο κλειδιά: ένα **δημόσιο κλειδί** και ένα **ιδιωτικό κλειδί**. Το ένα κλειδί, το δημόσιο διανέμεται και μπορεί να το έχει στην κατοχή του οποιοσδήποτε ενώ το ιδιωτικό όχι. Αυτά έχουν τις εξής ιδιότητες:

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

- Τα κλειδιά πρέπει δημιουργούνται σε ζευγάρια και πρέπει να είναι υπολογιστικά ανέφικτο να βρεθεί το ένα κλειδί από το άλλο.
- Κείμενο το οποίο έχει κρυπτογραφηθεί με το ένα κλειδί μπορεί να αποκρυπτογραφηθεί μόνο από το άλλο κλειδί του ζευγαριού και κείμενο που αποκρυπτογραφείται από το ένα κλειδί μπορεί να έχει κρυπτογραφηθεί μόνο από το άλλο κλειδί του ζευγαριού.

Προτάθηκε αρχικά το 1976 από δυο αμερικανούς ερευνητές, τον Whitfield Diffie και τον Martin Hellman, ως ένας τρόπος για να μην υπάρχει η ανάγκη μετάδοσης του κλειδιού ανάμεσα σε δυο πλευρές όπως συμβαίνει στην κρυπτογραφία συμμετρικού κλειδιού. Οι λεπτομέρειες της μεθόδου είναι πολύπλοκες και απαιτούν αρκετές γνώσεις μαθηματικών, συνεπώς το μόνο που μπορούμε να πούμε εδώ είναι ότι βασίστηκε αρχικά στο γεγονός ότι το να βρεθούν οι πρώτοι παράγοντες αριθμών μεγαλύτερων από π.χ. 10^{100} είναι υπολογιστικά δύσκολο που είναι σχεδόν απίθανο να γίνει.

Ο παραλήπτης ενός μηνύματος που χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού χρησιμοποιεί δυο κλειδιά με τον ακόλουθο τρόπο:

- Δημοσιοποιεί το δημόσιο κλειδί του π.χ. σε ένα site.
- Οποιοσδήποτε θέλει να στείλει μήνυμα στον κάτοχο του κλειδιού αυτού χρησιμοποιεί το δημόσιο κλειδί για να κάνει την κρυπτογράφηση.
- Το κρυπτογραφημένο κείμενο αποκρυπτογραφείται από τον παραλήπτη που εφαρμόζει τον κατάλληλο αλγόριθμο αποκρυπτογράφησης χρησιμοποιώντας το ιδιωτικό κλειδί.

Με αυτό τον τρόπο δεν χρειάζεται ο παραλήπτης να δημοσιοποιήσει το κλειδί που χρησιμοποιείται για αποκρυπτογράφηση. Αξίζει σε αυτό το σημείο να συγκρίνουμε τις δυο μεθόδους κρυπτογράφησης πριν εξετάσουμε μερικές τεχνολογίες δημοσίου κλειδιού και τις επιθέσεις που έχουν αυτές δεχτεί:

- Όταν χρησιμοποιούνται αρκετά μεγάλα κλειδιά και οι δυο μέθοδοι είναι ασφαλείς.
- Η κρυπτογραφία δημοσίου κλειδιού είναι ευκολότερο να υλοποιηθεί γιατί δεν χρειάζεται να ανησυχούμε για την μετάδοση κλειδιών μέσω ενός ανασφαλούς δικτύου.
- Η υπολογιστική ισχύς που χρειάζεται για κρυπτογραφία δημοσίου κλειδιού είναι πολύ μεγαλύτερη από αυτή που χρειάζεται για κρυπτογραφία συμμετρικού κλειδιού. Αυτό σημαίνει ότι για μεταφορά μεγάλων ποσοτήτων δεδομένων προτιμούνται συνήθως οι μέθοδοι

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

συμμετρικού κλειδιού.

Η Sarah Flannery και η κρυπτογραφία δημοσίου κλειδιού

Υπήρξαν διάφορες βελτιώσεις στον τομέα της κρυπτογραφίας δημοσίου κλειδιού τα τελευταία χρόνια. Μια ιδιαίτερα σημαντική ήταν αυτή που οφείλεται στην σε ένα δεκαεξάχρονο κορίτσι από την Ιρλανδία την Sarah Flannery, η οποία ανέπτυξε μια τεχνική που είναι περίπου 30 φορές γρηγορότερη από την αντίστοιχη προηγούμενη της που χρησιμοποιούνταν ευρέως στα συστήματα δημοσίου κλειδιού. Ωστόσο, παρότι το επίτευγμα της ήταν ιδιαίτερα σημαντικό, ακόμη υπάρχει μια μεγάλη διαφορά στις ανάγκες υπολογιστικής ισχύος μεταξύ των μεθόδων δημοσίου και συμμετρικού κλειδιού.

3.4.2 Τεχνολογίες

Υπάρχουν διάφορες τεχνολογίες και υλοποιήσεις της κρυπτογραφίας δημοσίου κλειδιού.

Ορισμένα άλλα δύσκολά υπολογιστικά προβλήματα προτάθηκαν για κρυπτογραφία δημοσίου κλειδιού. Όμως η ανάλυση ενός μεγάλου αριθμού άντεξε στο χρόνο και είναι η ιδέα πίσω από την κρυπτογραφία δημοσίου κλειδιού.

Έξυπνες κάρτες, ιδιωτικά και δημόσια κλειδιά

Ένας από τους πιο ασφαλείς τρόπους για να διασφαλιστεί η προστασία ενός ιδιωτικού κλειδιού είναι να το αποθηκεύσουμε σε μια έξυπνη κάρτα. Αυτές έχουν μέγεθος πιστωτικής κάρτας και περιέχουν και το ιδιωτικό και το δημόσιο κλειδί. Μπορούν να συνδεθούν σε ένα υπολογιστή και να στείλουν το ιδιωτικό κλειδί στον υπολογιστή ώστε αυτός να εκτελέσει την κρυπτογράφηση. Αυτό σημαίνει ότι το ιδιωτικό κλειδί δεν χρειάζεται ποτέ να αποθηκευθεί στον υπολογιστή και ότι όποιος θέλει να αποκτήσει το ιδιωτικό κλειδί πρέπει να κλέψει την κάρτα. ~~α~~Ακόμη κι έτσι όμως μπορεί να μην είναι δυνατόν να χρησιμοποιήσει το ιδιωτικό κλειδί καθώς οι έξυπνες κάρτες μπορούν να προγραμματιστούν ώστε να ζητάνε ένα κωδικό πριν δώσουν το δημόσιο κλειδί.

Η πρώτη τεχνολογία που θα εξετάσουμε είναι η **ανταλλαγή κλειδιού Diffie-Hellman**. Αυτή είναι μια τεχνική για την ανταλλαγή ενός συμμετρικού κλειδιού χρησιμοποιώντας δημόσιο κλειδί. Οι δυο πλευρές που συμμετέχουν

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

σε αυτή τη διαδικασία ανταλλάζουν αρχικά πληροφορίες σχετικά με κάποιο συμμετρικό κλειδί χρησιμοποιώντας μεθόδους δημοσίου κλειδιού και στη συνέχεια χρησιμοποιούν το συμφωνηθέν κλειδί για να επικοινωνήσουν.

Το **RSA** είναι σίγουρα το πιο γνωστό σύστημα σύστημα κρυπτογράφησης δημοσίου κλειδιού. Αναπτύχθηκε από τρεις καθηγητές στο MIT: τον Ronald Rivest, τον Adi Shamir και τον Leonard Adelman. το RSA μπορεί να χρησιμοποιηθεί για την αποστολή δεδομένων μέσω μιας μη ασφαλούς γραμμής και μπορεί επίσης να χρησιμοποιηθεί για τη δημιουργία ψηφιακών υπογραφών: σειρών χαρακτήρων δηλαδή που πιστοποιούν ότι ο αποστολέας του μηνύματος είναι αυτός που ισχυρίζεται πως είναι.

Το σύστημα **ElGamel sytem** είναι ένα σύστημα δημοσίου κλειδιού που βασίζεται στην ανταλλαγή κλειδιου Diffie-Hellman. Μπορεί επίσης να χρησιμοποιηθεί για ψηφιακές υπογραφές.

Το **Digital Signature Standard**, γνωστό ως DSS, αναπτύχθηκε από της αμερικανική εθνική υπηρεσία ασφάλειας και υιοθετήθηκε ως πρότυπο από την αμερικανική εθνική υπηρεσία τυποποιήσεων. Στην αρχική του μορφή μπορεί να χρησιμοποιηθεί μόνο για ψηφιακές υπογραφές, ωστόσο μπορεί να τροποποιηθεί για κανονική μεταφορά δεδομένων. Η τεχνική αυτή βασίζεται στον αλγόριθμο **Digital Signature Algorithm**.

3.4.3 Επιθέσεις σε συστήματα δημοσίου κλειδιού

Formatted: Font: (Default) Arial

Υπάρχουν δυο είδη επιθέσεων σε συστήματα δημοσίου κλειδιού. Η πρώτη είναι επίθεση με δεδομένα (**factoring attack)**. Πρωτύτερα στο κεφάλαιο αναφέρθηκε ότι οι γνωστές μέθοδοι κρυπτογραφίας δημοσίου κλειδιού βασίζονται στην τεράστια δυσκολία επίλυσης αντεστραμμένων προβλημάτων. Όποιος μπορεί να αναλύσει μεγάλους αριθμούς μπορεί να σπάσει και ένα σύστημα δημοσίου κλειδιού βασιζόμενος σε ανάλυση. Αυτό δεν είναι απίθανο: μαθηματικοί που δουλεύουν στην περιοχή την θεωρίας αριθμών έχουν μελετήσει προβλήματα ανάλυσης για καιρό και είναι πετυχημένοι με αριθμούς που έχουν συγκεκριμένα χαρακτηριστικά.

Η επίθεση RSA-129

Η πιο διάσημη επίθεση ανάλυσης έγινε στον αριθμό RSA-129 (129 ψηφία). Αυτός ο μεγάλος αριθμός παρουσιάστηκε σε ένα τεύχος του περιοδικού *Popular Science* το 1977. Τελικά αναλύθηκε από μια ομάδα ερευνητών υπό τον Arjen Lenstra.

Formatted: Right: 0,63 cm

Η άλλη τεχνική που εφαρμόζεται για το σπάσιμο μιας κρυπτογραφίας δημοσίου κλειδιού είναι να βρεθεί κάποιο μειονέκτημα στον αλγόριθμο που χρησιμοποιείται. Για παράδειγμα, ένα από τα πρώτα προβλήματα που παρουσιάστηκαν είναι το knapsack. Βρέθηκε ότι είναι εύκολο να εξακριβωθεί το ιδιωτικό κλειδί από το δημόσιο κλειδί σε ένα σύστημα με αυτό το πρόβλημα.

Κρυπτογραφία ελλειπτικής καμπύλης.

Μια πολλά υποσχόμενη μορφή κρυπτογραφίας που απειλεί να ξεπεράσει τη χρήση ανάλυσης στα συστήματα δημοσίου κλειδιού είναι η κρυπτογραφία ελλειπτικής καμπύλης. περιλαμβάνει την επίλυση δύσκολων υπολογιστικά προβλημάτων χρησιμοποιώντας μια οικογένεια καμπυλών, γνωστές σαν ελλειπτικές καμπύλες. Πολλά συστήματα δημοσίου κλειδιού χρησιμοποιούν τον RSA. Παρόλα αυτά, η αυξανόμενη ισχύς των υπολογιστών έφερε και την αύξηση του μήκους των bit, που οδήγησε σε ακόμη μεγαλύτερες υπολογιστικές απαιτήσεις. Η κρυπτογραφία ελλειπτικής καμπύλης είναι το ίδιο ασφαλή με τον RSA. Όμως, απαιτεί μικρότερα μήκη bit και συνεπώς λιγότερους υπολογισμούς.

3.5 Συναρτήσεις ανασκόπησης μηνύματος (message digest)

Formatted: Font: (Default) Arial

Αυτές είναι μαθηματικές συναρτήσεις που όταν εφαρμοστούν σε ένα αρχείο επιστρέφουν έναν αριθμό γνωστό ως **ανασκόπηση** που με κάποιο τρόπο παρέχει ένα περίπου μοναδικό τρόπο προσδιορισμού του αρχείου. Ένα παράδειγμα μιας ιδιαίτερα αναποτελεσματικής συνάρτησης ανασκόπησης μηνύματος θα ήταν να παίρνουμε κάθε χαρακτήρα του αρχείου με τη σειρά, να προσθέτουμε τους κωδικούς bit τους με τη σειρά και τέλος να παίρνουμε το υπόλοιπο της διαίρεσης του αριθμού αυτού με ένα πολύ μεγάλο αριθμό. Μια συνάρτηση ανασκόπησης μηνύματος θα πρέπει να έχει τα εξής χαρακτηριστικά:

- Κάθε κομμάτι της εισόδου στη συνάρτηση θα πρέπει να επηρεάζει το αποτέλεσμα.
- Αν κάποιο bit στην είσοδο της συνάρτησης ανασκόπησης μηνύματος μεταβληθεί, τότε κάθε bit στο αποτέλεσμα της συνάρτησης θα έχει πιθανότητα 0.5 να αλλάξει.
- Θα πρέπει να είναι υπολογιστικά ανέφικτο να βρεθεί κάποιο αρχείο το οποίο δίνει το ίδιο αποτέλεσμα όταν εισαχθεί στη συνάρτηση με ένα

Formatted: Right: 0,63 cm

άλλο αρχείο.

Υπάρχουν διάφορες χρήσεις αυτών των συναρτήσεων~~, θα εξετάσουμε μια συγκεκριμένη, την ψηφιακή υπογραφή, αργότερα στο κεφάλαιο αυτό~~. Ωστόσο, μια άλλη χρήση τους είναι να ανακαλύψουμε αν κάποιο αρχείο στο σύστημα έχει μεταβληθεί, είτε από έναν εισβολέα είτε από έναν ιό. Στα πρώτα χρόνια που εμφανίστηκαν οι ιοί, κανείς μπορούσε να τους εντοπίσει απλά κοιτώντας το μέγεθος σε bytes του κώδικα. Ωστόσο, οι κατασκευαστές ιών κατάφεραν να παρακάμψουν αυτό το εμπόδιο είτε φτιάχνοντας ιούς οι οποίοι κόβουν χρήσιμο κώδικα από υπάρχοντα προγράμματα και τοποθετούν τον εαυτό τους μέσα με τέτοιο τρόπο ώστε το μέγεθος του αρχείου φαίνεται ακριβώς το ίδιο, είτε παραπλανώντας το ίδιο το λειτουργικό σύστημα και το σύστημα αρχείων σχετικά με το πραγματικό μέγεθος του αρχείου. Ένας τρόπος να εντοπιστούν αλλαγές σε αρχεία είναι να συγκριθεί το αποτέλεσμα της συνάρτησης ανασκόπησης του αρχείου με την προηγούμενη (αποθηκευμένη) τιμή. Αν είναι ίδια τότε είναι σχεδόν απολύτως σίγουρο ότι το αρχείο δεν τροποποιήθηκε αλλά αν δεν είναι τότε το αρχείο σίγουρα έχει αλλάξει.

Υπάρχει μια σειρά συναρτήσεων ανασκόπησης μηνύματος και σχετικών τεχνολογιών που έχουν αναπτυχθεί:

- *HMAC*. Αυτή είναι μια τεχνική που χρησιμοποιείται για να ελέγχεται αν κάποιο αρχείο έχει τροποποιηθεί. Χρησιμοποιεί και μια συνάρτηση ανασκόπησης μηνύματος και ένα ιδιωτικό κλειδί. Μια συνάρτηση ανασκόπησης μηνύματος χρησιμοποιείται στο κείμενο, κρυπτογραφείται και στέλνεται με το κείμενο. Ο παραλήπτης αποκρυπτογραφεί την ανασκόπηση του μηνύματος, χρησιμοποιεί τη συνάρτηση ανασκόπησης πάνω στο κείμενο και συγκρίνει τα δυο αποτελέσματα. Αν συμφωνούν τότε το μήνυμα έφτασε ασφαλές.
- *Η σειρά MD*. Αυτή είναι μια σειρά συναρτήσεων ανασκόπησης μηνύματος που αναπτύχθηκε από τον Ronald Rivest. Όλες παράγουν ως αποτέλεσμα έναν αριθμό των 128 bit. Διαφέρουν μεταξύ τους όσον αφορά την ταχύτητα με την οποία μπορούν να υπολογιστούν και την ισχύ της συνάρτησης: το πόσο εύκολο είναι να ανακαλύψει κανείς ένα αρχείο που δίνει το ίδιο αποτέλεσμα με ένα άλλο..
- *Η σειρά SHA*. Αυτές οι συναρτήσεις ανασκόπησης μηνύματος αναπτύχθηκαν από την αμερικανική εθνική υπηρεσία ασφαλείας.

Formatted: Right: 0,63 cm

Παράγουν αποτέλεσμα μεγέθους 160 bit.

Υπάρχουν και άλλες χρήσεις των συναρτήσεων ανασκόπησης μηνύματος εκτός από τον έλεγχο αρχείων για παραποίηση. Χρησιμοποιούνται επίσης για **κώδικες πιστοποίησης μηνύματος**. Σε αυτή την χρήση υπολογίζεται το αποτέλεσμα της συνάρτησης για ένα μήνυμα το οποίο στέλνεται από κάποιον αποστολέα σε κάποιον παραλήπτη και στη συνέχεια επισυνάπτεται στο τέλος του μηνύματος. Και οι δυο πλευρές πρέπει να χρησιμοποιούν την ίδια συνάρτηση ανασκόπησης μηνύματος. Ο αποστολέας θα τη χρησιμοποιήσει για να υπολογίσει τον αριθμό που πρέπει να επισυνάψει στο μήνυμα και ο παραλήπτης θα την χρησιμοποιήσει για να υπολογίσει τον αριθμό ανασκόπησης του μηνύματος που παρέλαβε. Αν η τιμή που υπολόγισε ο παραλήπτης είναι ίδια με αυτή που υπήρχε στο τέλος του μηνύματος, τότε είναι πολύ πιθανό πως δεν υπήρξε παραποίηση του μηνύματος καθώς αυτό διέσχιζε το τηλεπικοινωνιακό δίκτυο.

Άλλη μια χρήση των συναρτήσεων ανασκόπησης μηνύματος είναι η παραγωγή ενός password από μια σειρά λέξεων γνωστή ως **passphrase**. Ένα απλό και αφελές παράδειγμα είναι να θυμάστε το password itbilhpway από τη φράση 'In the beginning I liked hash potatoes, what about you'. Η συνάρτηση παίρνει απλά το πρώτο γράμμα κάθε λέξης. Έτσι ο χρήστης μπορεί να θυμάται ένα σχετικά δύσκολο password. Οι συναρτήσεις ανασκόπησης μηνύματος χρησιμοποιούνται επίσης σε ψηφιακές υπογραφές, αυτές εξετάζονται στην επόμενη ενότητα.

3.6 Ψηφιακές υπογραφές

Formatted: Font: (Default) Arial, 14 pt

Μια ψηφιακή υπογραφή είναι κάποια δεδομένα τα οποία με μοναδικό τρόπο προσδιορίζουν κάποιο άτομο ή οργανισμό. Οι ψηφιακές υπογραφές βασίζονται σε συναρτήσεις ανασκόπησης μηνύματος και κρυπτογραφία δημοσίου κλειδιού. Για να περιγράψουμε πως λειτουργούν σκεφτείτε την αποστολή από ένα ~~άτομα~~ άτομο Α σε ένα άλλο άτομο Β όπου το άτομο Α έχει γνωστοποιήσει το δημόσιο κλειδί του. Υποθέτουμε ότι και οι δυο πλευρές χρησιμοποιούν την ίδια συνάρτηση ανασκόπησης μηνύματος. Τα παρακάτω βήματα γίνονται:

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

- Το άτομο Α υπολογίζει το αποτέλεσμα της συνάρτησης ανασκόπησης μηνύματος στο μήνυμα που θέλει να στείλει.
- Το αποτέλεσμα κρυπτογραφείται χρησιμοποιώντας το ιδιωτικό κλειδί.

Formatted: Right: 0,63 cm

Αυτή είναι η ψηφιακή υπογραφή.

- Το μήνυμα μαζί με την ψηφιακή υπογραφή στέλνεται στο άτομο Β.
- Ο Β αποκρυπτογραφεί την ψηφιακή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί του Α για να πάρει τον αριθμό ανασκόπησης μηνύματος.
- Ο Β στη συνέχεια υπολογίζει το αποτέλεσμα της συνάρτησης ανασκόπησης μηνύματος (ίδια με αυτή που χρησιμοποίησε ο Α) και το συγκρίνει με την αποκρυπτογραφημένη τιμή. αν ταιριάζουν το μήνυμα έχει σταλεί πράγματι από τον κάτοχο του κλειδιού που χρησιμοποιήθηκε.

Ένα σημαντικό στοιχείο είναι ότι οι ψηφιακές υπογραφές παρέχουν ακράδαντες αποδείξεις αν κάποιο μήνυμα παραποιήθηκε κατά τη μεταφορά του ή όχι αλλά δεν κρύβουν το μήνυμα που στάλθηκε και συνεπώς δεν είναι κατάλληλες από μόνες τους όταν απαιτείται προστασία ανάγνωσης του περιεχομένου του μηνύματος από τρίτους.

3.7 Ψηφιακά πιστοποιητικά

Formatted: Font: (Default) Arial, 14 pt

Formatted: Font: (Default) Arial

Ένα πρόβλημα με τα συστήματα δημοσίου κλειδιού είναι ότι ενώ παρέχουν τη δυνατότητα ασφαλούς επικοινωνίας δεν είναι από μόνα τους κατάλληλα για ασφαλή ελεύθερη δημόσια επικοινωνία. Ο λόγος είναι ότι δεν υπάρχει τρόπος να πιστοποιηθεί σε ένα εντελώς ανοιχτό περιβάλλον ότι κάποιο άτομο το οποίο ισχυρίζεται ότι έχει ένα συγκεκριμένο κλειδί είναι πράγματι αυτός που λέει. Για παράδειγμα κάποιος ο οποίος υποστηρίζει ότι έχει το κλειδί που αντιστοιχεί στον πρωθυπουργό ενώ δεν είναι θα μπορεί να διαβάζει μηνύματα τα οποία κάποιοι άλλοι νομίζουν ότι στέλνουν στον πρωθυπουργό.

Το πρότυπο x509.v3

Πιθανόν το πιο διαδεδομένο πρότυπο για ψηφιακά πιστοποιητικά είναι το x509.v3. Αυτό περιέχει όλα τα στοιχεία σχετικά με τις ψηφιακές υπογραφές που θα αναφερθούν παρακάτω, ωστόσο περιγράφει επίσης την δυνατότητα να περιλαμβάνονται στο πιστοποιητικό ζευγάρια ονόματος / τιμής που βοηθούν την πιστοποίηση. Για παράδειγμα, ένα πιστοποιητικό το οποίο έχει οριστεί βάσει αυτού του προτύπου μπορεί να περιέχει και πληροφορίες σχετικά με το ποια συνάρτηση ανασκόπησης μηνύματος

Formatted: Right: 0,63 cm

χρησιμοποιήθηκε για να δημιουργήσει την ψηφιακή υπογραφή του πιστοποιητικού.

Για να ξεπεραστεί το πρόβλημα αυτό, έχουν αναπτυχθεί τα **ψηφιακά πιστοποιητικά.** Ένα ψηφιακό πιστοποιητικό είναι ένα έγγραφο που εκδίδεται από έναν έμπιστο οργανισμό όπως για παράδειγμα τα εθνικά ταχυδρομεία μιας χώρας και που δίνει στοιχεία για έναν χρήστη. Το πιστοποιητικό θα περιέχει στοιχεία όπως το όνομα του χρήστη, ένας μοναδικός σειριακός αριθμός και φυσικά το δημόσιο κλειδί του. Το πιστοποιητικό θα έχει επίσης και μια ψηφιακή υπογραφή του οργανισμού που το εξέδωσε. Για πιστοποιήσει την αυθεντικότητα ενός ψηφιακού πιστοποιητικού, ο παραλήπτης ενός μηνύματος θα πρέπει να έχει το δημόσιο κλειδί του έμπιστου οργανισμού που το εξέδωσε. Συχνά, πολλά από τα κλειδιά μεγάλων δημοσίων οργανισμών περιλαμβάνονται σε προγράμματα όπως οι browsers.
Αφού έχει ληφθεί ένα πιστοποιητικό, αυτό που πρέπει να κάνει κάποιος για να πιστοποιήσει ότι αυτό αντιστοιχεί πραγματικά στο άτομο ή τον οργανισμό που νομίζει είναι να ακολουθήσει την παρακάτω διαδικασία:

- Ελέγχει ότι η υπογραφή του πιστοποιητικού από την υπηρεσία πιστοποίησης είναι έγκυρη χρησιμοποιώντας το δημόσιο κλειδί της υπηρεσίας πιστοποίησης. Πολλές φορές αυτό θα υπάρχει στον browser. Αν δεν υπάρχει θα πρέπει να ανακτηθεί μέσω μιας σειράς ιεραρχικής αναζήτησης από αρχές πιστοποίησης που ήδη γνωρίζουμε.
- Χρησιμοποιεί το δημόσιο κλειδί που υπάρχει στο ψηφιακό πιστοποιητικό για να κρυπτογραφήσει δεδομένα που θέλει να στείλει στον κάτοχο του πιστοποιητικού. Κάποιες φορές τα δεδομένα μπορεί απλά να είναι ένα κλειδί το οποίο θα χρησιμοποιηθεί στη συνέχεια μεταξύ των δυο πλευρών για επικοινωνία μέσω κάποιας απλούστερης μεθόδου συμμετρικού κλειδιού.

Ένα πρακτικό παράδειγμα αποτελούν τα ψηφιακά πιστοποιητικά που σχετίζονται με μια πολύ δημοφιλή τεχνολογία γνωστή ως Secure Sockets Layer (SSL) και η οποία θα περιγραφεί αργότερα. Το SSL συνήθως χρησιμοποιείται για την αποστολή κρυπτογραφημένων μηνυμάτων μεταξύ ενός browser και ενός server,π.χ. για αποστολή στοιχείων πιστωτικών καρτών..
Όταν ένας browser συνδέεται με έναν Web server που χρησιμοποιεί SSL, το πρώτο πράγμα που συμβαίνει είναι ότι ο server στέλνει στον browser ένα

Formatted: Right: 0,63 cm

ψηφιακό πιστοποιητικό τύπου x509.v3 το οποίο περιλαμβάνει το δημόσιο κλειδί του server. Ο browser τότε ελέγχει την εγκυρότητα του πιστοποιητικού εξετάζοντας την ψηφιακή υπογραφή την οποία φέρει. Αν ο έλεγχος είναι επιτυχής, τότε το δημόσιο κλειδί που υπάρχει μέσα στο πιστοποιητικό χρησιμοποιείται για την αποκωδικοποίηση των αρχικών πληροφοριών που στέλνει ο server για να γίνει η αρχική εγκατάσταση της σύνδεσης. Η αρχική εγκατάσταση της σύνδεσης περιλαμβάνει και κάποια συμφωνία για το πως θα γίνει στη συνέχεια η επικοινωνία μεταξύ των δυο πλευρών. Για παράδειγμα ότι θα χρησιμοποιηθεί κρυπτογραφία συμμετρικού κλειδιού. Ο λόγος για τον οποίο μπορεί να χρησιμοποιηθεί κρυπτογραφία συμμετρικού κλειδιού είναι ότι η επικοινωνία μπορεί να απαιτεί μεταφορά μεγάλου όγκου δεδομένων και συνεπώς η κρυπτογράφηση και αποκρυπτογράφηση δημοσίου κλειδιού μπορεί να είναι υπερβολικά αργή.

Υπάρχουν τέσσερα είδη ψηφιακών υπογραφών που χρησιμοποιούνται στο Internet. Όλα ακολουθούν το πρότυπο x509.v3.

- *Πιστοποιητικά αρχών πιστοποίησης*. Αυτά χρησιμοποιούνται για την πιστοποίηση μια αρχής πιστοποίησης όπως ταχυδρομικά γραφεία, οργανισμοί τηλεπικοινωνιών κ.λ.π., που μπορούν να εκδώσουν ψηφιακά πιστοποιητικά.
- *Πιστοποιητικά Server*. Αυτά πιστοποιούν ένα server και αποδεικνύουν ότι είναι αυτός που ισχυρίζεται ότι είναι. Αυτά τα πιστοποιητικά χρησιμοποιούνται σε συνδυασμό με κάποια άλλη τεχνολογία όπως το SSL.
- *Προσωπικά πιστοποιητικά*. Αυτά πιστοποιούν ξεχωριστά άτομα.
- *Πιστοποιητικά εταιρειών λογισμικού*. Αυτά χρησιμοποιούνται για να πιστοποιούν προγράμματα τα οποία πωλούνται και διανέμονται.

3.8 Ανταλλαγή κλειδιών

Formatted: Font: (Default) Arial, 14 pt, Not Highlight

Μια χρήση της κρυπτογραφίας δημοσίου κλειδιού είναι στην μετάδοση μιας μυστικής πληροφορίας όπως ένα κλειδί που χρησιμοποιείται σε ένα συμμετρικό σύστημα. Ένα παράδειγμα είναι το **σύστημα ανταλλαγής κλειδιών των Diffie-Hellman**. Αυτή είναι μια τεχνική που χρησιμοποιείται για να προστατέψει ένα κλειδί που χρησιμοποιείται σε συμμετρικά συστήματα. Με αυτό, οι δυο πλευρές που πρόκειται να επικοινωνήσουν πρώτα ανταλλάσσουν πληροφορίες για το συμμετρικό κλειδί χρησιμοποιώντας

Formatted: Font: (Default) Arial, Not Highlight

Formatted: Right: 0,63 cm

κρυπτογραφία δημοσίου κλειδιού.

3.9 Ψηφιακοί Φάκελοι (Digital Envelopes)

Ο μηχανισμός των ψηφιακών φακέλων βρίσκει εφαρμογή στην ανταλλαγή μυστικών κλειδιών που χρησιμοποιούνται σε συμμετρικά κρυπτοσυστήματα. Ο ψηφιακός φάκελος αποτελείται από ένα μήνυμα κρυπτογραφημένο με ένα συμμετρικό κλειδί και το συμμετρικό κλειδί κρυπτογραφημένο με άλλο κλειδί. Συνήθως η κρυπτογράφηση του συμμετρικού κλειδιού γίνεται με την δημόσια κλείδα της αντίθετης πλευράς, αλλά αυτό δεν είναι απαραίτητο. Μπορεί κάλλιστα να χρησιμοποιηθεί και ένα προσυμφωνημένο συμμετρικό κλειδί.

Ας υποθέσουμε ότι ο χρήστης Β θέλει να στείλει μήνυμα στον χρήστη Β. Ο Α διαλέγει ένα συμμετρικό κλειδί και κρυπτογραφεί το μήνυμα με αυτό. Έπειτα κρυπτογραφεί το μυστικό συμμετρικό κλειδί με την δημόσια κλείδα του Β. Στέλνει στον Β το κρυπτογραφημένο μήνυμα συνοδευόμενο από το κρυπτογραφημένο κλειδί. Όταν ο Β θελήσει να διαβάσει το μήνυμα, χρησιμοποιεί την ιδιωτική του κλείδα για να ανακτήσει το συμμετρικό κλειδί και μετά αποκρυπτογραφεί το μήνυμα με το μυστικό συμμετρικό κλειδί. Στην περίπτωση που το μήνυμα έχει παραπάνω του ενός παραλήπτες, το μυστικό συμμετρικό κλειδί κρυπτογραφείται ξεχωριστά με την δημόσια κλείδα του κάθε παραλήπτη. Και πάλι μεταδίδεται ένα κρυπτογραφημένο μήνυμα.

Οι χρήστες μπορούν να αλλάζουν κλειδιά όσο συχνά θέλουν, γεγονός που αυξάνει κατακόρυφα την ασφάλεια του συστήματος. Επίσης, οι ψηφιακοί φάκελοι όχι μόνο λύνουν το πρόβλημα της ανταλλαγής κλειδιών, αλλά βελτιώνουν και την απόδοση του συστήματος καθ' ότι η ασύμμετρη κρυπτογράφηση από μόνη της απαιτεί εξαιρετικά χρονοβόρα επεξεργασία. Ο πιο συνηθισμένος συνδυασμός είναι το ασύμμετρο κρυπτοσύστημα RSA με το συμμετρικό DES.

3.10 Στεγανογραφία (steganography)

Με αυτή την ελληνική λέξη περιγράφουμε την απόκρυψη του γεγονότος ότι κάποιο μήνυμα είναι κρυπτογραφημένο. Για παράδειγμα, δεν χρειάζεται μεγάλη φαντασία για να καταλάβει κανείς ότι το παρακάτω είναι ένα κρυπτογραφημένο μήνυμα:

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

Ξλμθψκλφ λπιρ

Αν ψάξετε λίγο θα δείτε ότι το μόνο που έκανα ήταν να μεταθέσω τα γράμματα κατά 8 θέσεις. Έτσι αντί για Χ έγραψα Ξ, αντί για Τ έγραψα Λ κ.ο.κ. (Η φράση είναι "Χτυπήστε Τώρα").

Στην απλή κρυπτογράφηση, πραγματοποιείται μια νοητική πάλη μεταξύ του κρυπτογράφου και του κρυπταναλυτή. Αν ο πρώτος είναι καλύτερος, το μήνυμα δεν θα διαβαστεί. Αν όμως υπερισχύσει ο δεύτερος, τότε όλα θα έρθουν στο φως.

Στην απλή κρυπτογραφία όμως, ο κρυπταναλυτής (π.χ. η αστυνομία) γνωρίζει ήδη μια πολύ σημαντική πληροφορία: Είναι φανερό ότι ο Α και ο Β χρησιμοποιούν κώδικα για τις επικοινωνίες τους, άρα έχουν κάτι να κρύψουν. Πρέπει λοιπόν να αρχίσει να τους παρακολουθεί στενά.

Διαφορετική είναι η κατάσταση στο ακόλουθο μήνυμα:

Χωρίς τα υπόλοιπα, που ήταν σε τελικό έλεγχο, τέσσερις ώρες ρύθμιση αρκούσαν.

Προσέξτε ότι τα πρώτα γράμματα των λέξεων σχηματίζουν και εδώ τη φράση "Χτυπήστε Τώρα". Ωστόσο, αυτό το μήνυμα είναι κρυμμένο μέσα σε μια αθώα φράση και μόνο ένας ειδικά εκπαιδευμένος άνθρωπος θα υποπτευόταν κάτι διαβάζοντάς την. Ακόμη και αυτός όμως μάλλον δεν θα έβρισκε άκρη αν συναντούσε το:

Ξέρεις, λέω μαζί θα ψάξουμε καλύτερα. Λίγες φορές λάθεψα πολύ. Ίσως ρυθμίστηκαν.

Εδώ τα πρώτα γράμματα των λέξεων σχηματίζουν την κρυπτογραφημένη ακολουθία χαρακτήρων "Ξλμθψκλφ λπιρ". Εννοείται ότι τα παραπάνω παραδείγματα είναι πολύ απλοϊκά και χρησιμοποιήθηκαν απλώς για να εξηγήσουν τι σημαίνει στεγανογραφία (ενσωμάτωση ενός μηνύματος μέσα σε ένα άλλο). Στην πραγματικότητα, τα κρυπτογραφημένα μηνύματα συνήθως δεν ενσωματώνονται μέσα σε κείμενο, αλλά σε ξεχωριστά αρχεία (π.χ. σε φωτογραφίες). Έτσι, ο Α μπορεί να στείλει στον Β μια αθώα φωτογραφία από τις διακοπές του, αλλά μέσα στα bits που την αποτελούν να βρίσκεται κρυμμένο το μήνυμα που θέλει να του μεταδώσει.

Δυστυχώς για τις διωκτικές αρχές, ακόμη και απλές τεχνικές όπως οι παραπάνω είναι αρκετές για να ξεγελάσουν τα αυτόματα μηχανήματα ανίχνευσης (dictionary computers) και μπορούν να αναγνωριστούν μόνο από ειδικά εκπαιδευμένους ανθρώπους.

Formatted: Right: 0,63 cm

Επειδή όμως οι τελευταίοι δεν μπορούν να διαβάζουν όλα τα μηνύματα που κυκλοφορούν στο Internet, όλα δείχνουν ότι η τεχνολογία δεν μπορεί να απαντήσει μόνη της στο πρόβλημα της τρομοκρατίας. Για το ορατό μέλλον λοιπόν, η κατασκοπία και η αντικατασκοπία θα συνεχίσουν να βασίζονται στις παραδοσιακές ανθρωποκεντρικές μεθόδους συλλογής πληροφοριών (κατάσκοποι, πληροφοριοδότες κ.λπ.).

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

ΚΕΦΑΛΑΙΟ 4

ΜΟΝΤΕΛΑ ΑΣΦΑΛΕΙΑΣ

Formatted: Indent: First line: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

~~4.1 Η Προσέγγιση~~

Formatted: Font: (Default) Arial, 14 pt, Not Italic

Formatted: Font: (Default) Arial, 14 pt

4.1~~.1~~ Γενικά

Formatted: Font: (Default) Arial, 14 pt

Για την κατάταξη των νέων πρωτοκόλλων και συστημάτων που, είναι απαραίτητη η υιοθέτηση ενός μοντέλου, σαν αυτό του OSI, που θα βοηθήσει στην κατανόηση της λειτουργικότητας των και της συσχέτισης τους τόσο μεταξύ τους, όσο και με τα πρωτόκολλα του Internet. Η προσέγγιση μας βασίστηκε στο πολυεπίπεδο μοντέλο που ακολουθεί και προσομοιάζει τα επίπεδα του Διαδικτύου.

Formatted: Font: (Default) Arial

4.~~1.~~2 Το Μοντέλο

Formatted: Left, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, 14 pt

Formatted: Font: (Default) Arial, 14 pt

5.	*APPLICATIONS*
4.	*INTERNET SERVICES*
3.	*HIGHER INTERNET PROTOCOLS*
2.	*TCP/IP*
1.	*NETWORK ACCESS*

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

4.1.3 Σύντομη Περιγραφή του Μοντέλου

Στο πρώτο επίπεδο του μοντέλου ασφαλείας, περιλαμβάνονται οι τεχνικές ασφάλισης του ηλεκτρικού σήματος. Οι τεχνικές αυτές έχουν να κάνουν με την κωδικοποίηση των bits για μετάδοση στο μέσο, την πολυπλεξία λογικών καναλιών με την χρήση διαφορετικών συχνοτήτων και τα bits ισοτιμίας. Οι τεχνικές διαφέρουν ανάλογα με την τεχνολογία τοπικών δικτύων που χρησιμοποιείται (Ethernet, Token Ring, FDDI), ενώ παρόμοιες μέθοδοι εφαρμόζονται και από τα modem στις dial-up συνδέσεις. Συγκεκριμένα, η λειτουργία των modem βασίζεται σε πρωτόκολλα που καθορίζουν τους αλγόριθμους που υλοποιούνται σε τσιπ σιλικόνης. Σε αυτό το επίπεδο ανήκουν και οι περιπτώσεις της hardware κρυπτογραφίας και στεγανογραφίας.

Στο επίπεδο TCP/IP κατατάσσονται τα συστήματα που εξασφαλίζουν την επικοινωνία με τα πρωτοκόλλα TCP και IP. Παράδειγμα συστήματων αυτού του επιπέδου είναι IPSec και το NAT.

Στο αμέσως πιο πάνω επίπεδο, στο επίπεδο *HIGHER INTERNET PROTOCOLS* βρίσκουμε το SSL, πρωτόκολλο που στοχεύει στην διασφάλιση του πακέτου TCP/IP και των εφαρμογών που χρησιμοποιούν το TCP/IP. Το SSL προσθέτει δύο νέα επίπεδα στο OSI μοντέλο, γεγονός που το τοποθετεί ένα επίπεδο πάνω από το IPSec.

Στο επίπεδο των υπηρεσιών του Διαδικτύου ανήκουν όλα τα συστήματα που αποτελούν προεκτάσεις των υπαρχόντων πρωτοκόλλων υπηρεσιών, προσθέτοντας χαρακτηριστικά ασφαλείας. Οι υπηρεσίες που διασφαλίζονται είναι το ηλεκτρονικό ταχυδρομείο, το World Wide Web, το DNS και το remote login. Παράδειγμα αυτών των συστημάτων είναι το *S/MIME*, το *PEM*, το *S/HTTP*.

Τέλος, στο επίπεδο των εφαρμογών κατατάσσονται πιο ολοκληρωμένα συστήματα, που πολλές φορές χρησιμοποιούν πρωτόκολλα από το παρακάτω επίπεδο. Καλύπτουν πληθώρα αναγκών και συνήθως αναπτύσσονται από οργανισμούς για εσωτερική χρήση. Η επιτυχία του κάθε συστήματος καθορίζει της αποδοχή του από την κοινότητα του Διαδικτύου. Μερικά από αυτά είναι το *Kerberos*, το *S/KEY*, το *RADIUS*, ενώ υπάρχουν και πιο γενικές έννοιες όπως αυτή των *Firewalls*. Στα δύο τελευταία επίπεδα του

Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

μοντέλου ασφαλείας ανήκουν και τα περισσότερα από τα νέα πρωτόκολλα.

Στις σελίδες που ακολουθούν, θα επιχειρήσουμε να παρουσιάσουμε τα υπάρχοντα δικτυακά συστήματα ασφαλείας και συγχρόνως να τα κατατάξουμε σύμφωνα με το παραπάνω μοντέλο. Λόγω της φύσης των τεχνικών που χρησιμοποιούνται στο πρώτο επίπεδο, η οποίες ~~εξαρτούνται~~εξαρτώνται από την εκάστοτε τεχνολογία δικτύων, δεν θα αναφερθούμε καθόλου σε αυτό. Οι τεχνικές αυτές έχουν να κάνουν περισσότερο με τα χαρακτηριστικά της σύνδεσης και δεν έχουν γίνει προσπάθειες για την περαιτέρω διασφάλιση τους. Ακόμα, οι περιπτώσεις της hardware κρυπτογραφίας και στεγανογραφίας, δεν εφαρμόζεται παρά σε ελάχιστες, εξειδικευμένες καταστάσεις, όπως στις στρατιωτικές και κυβερνητικές επικοινωνίες.

Formatted: Line spacing: 1,5 lines

Formatted: Indent: First line: 0 cm, Line spacing: 1,5 lines

ΚΕΦΑΛΑΙΟ 5

ΚΑΤΑΤΑΞΗ ΔΙΚΤΥΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

~~α.~~5.1 SSL (Secure Socket Layer)

Formatted: Font: (Default) Arial, Not Highlight

Formatted: Indent: Left: 0 cm, First line: 0 cm, Line spacing: 1,5 lines, Outline numbered + Level: 2 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0,95 cm + Tab after: 1,59 cm + Indent at: 1,59 cm, Tab stops: 0 cm, List tab + Not at 1,59 cm + 2,8 cm

Το πρωτόκολλο SSL στοχεύει στην διασφάλιση της ~~μυστικότητας~~μυστικότητας (privacy) και της αξιοπιστίας (reliability) στην επικοινωνία μεταξύ δύο εφαρμογών. Αναπτύχθηκε από την Netscape Communications, υποβλήθηκε στο W3C ως πρόταση της εταιρίας για την υιοθέτηση του ως προτύπου, και είναι διαθέσιμο σε μορφή Internet Draft . Σχεδιάστηκε για την υποστήριξη πρωτοκόλλων επιπέδου εφαρμογής όπως τα HTTP, NNTP, FTP και Telnet. Αποτελείται από δύο επίπεδα (layers).

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Στο κατώτερο επίπεδο του SSL τοποθετείται το SSL Record Protocol. Το SSL Record Protocol προϋποθέτει για την λειτουργία του ένα αξιόπιστο πρωτόκολλο μεταφοράς όπως το TCP και χρησιμοποιείται για την ενθυλάκωση (encapsulation) πρωτοκόλλων υψηλότερου επιπέδου. Ενα από αυτά τα επίπεδα είναι το SSL Handshake Protocol. Το τελευταίο πρωτόκολλο επιτρέπει στον server και στον client να πιστοποιήσουν (authenticate) ο ένας

Formatted: Right: 0,63 cm

τον άλλο (κάνοντας χρήση digital signature και certificate) και να διαπραγματευτούν αλγόριθμο και κλειδιά κρυπτογράφησης. Η διαπραγμάτευση

αυτή γίνεται πριν την ανταλλαγή δεδομένων μεταξύ πρωτοκόλλων επιπέδου εφαρμογής. Το βασικό πλεονέκτημα του SSL είναι η ανεξαρτησία του από τα πρωτόκολλα αυτά.

Το πρωτόκολλο SSL παρέχει ασφάλεια σύνδεσης (connection security) η οποία έχει τρεις βασικές ιδιότητες:

• Η σύνδεση είναι ιδιωτική. Κρυπτογράφηση χρησιμοποιείται μετά από την αρχική χειραψία (handshake) για τον καθορισμό ενός μυστικού κλειδιού. Για την κρυπτογράφηση των δεδομένων χρησιμοποιούνται συμμετρικοί αλγόριθμοι όπως DES, RC4 κλπ.

• Η σύνδεση μπορεί να πιστοποιηθεί χρησιμοποιώντας μη-συμμετρικό αλγόριθμο κρυπτογράφησης (ή δημόσιου κλειδιού) όπως RSA, DSS κλπ..

• Η σύνδεση είναι αξιόπιστη Στην μεταφορά των μηνυμάτων περιλαμβάνεται έλεγχος εγκυρότητας (integrity check) με την χρήση αλγορίθμου MAC (Message Authenticity Check) βάσει κλειδιών (keyed MAC).

Μία SSL σύνοδος διαθέτει μνήμη (stateful session). Ο συντονισμός των καταστάσεων του client και του server αποτελεί ευθύνη του SSL Handshake Protocol. Μία σύνοδος μπορεί να περιέχει πολλαπλές ασφαλείς συνδέσεις. Το επίπεδο SSL Record δέχεται δεδομένα (μηνύματα) από τα ανώτερα στρώματα σε μη-κενά blocks που δεν έχουν κάποιο συγκεκριμένο μήκος. Τα blocks αυτά κερματίζονται (fragmentation) από το επίπεδο σε εγγραφές (SSLPlaintext records) μέγιστου μήκους 214 bytes. Πολλαπλά μηνύματα ανωτέρων πρωτοκόλλων μπορούν να συμπεριληφθούν σε μία τέτοια εγγραφή. Οι εγγραφές συμπιέζονται (προαιρετικά) κάνοντας χρήση του αλγορίθμου που έχει οριστεί στην τρέχουσα κατάσταση της συνόδου. Με την εφαρμογή της συμπίεσης οι SSLPlaintext εγγραφές μετασχηματίζονται σε SSLCompressed δομές. Η συμπίεση είναι lossless. Ο γενικός μηχανισμός λειτουργίας του SSL παρουσιάζεται στο σχήμα που ακολουθεί:

Formatted: Font: (Default) Arial, Greek

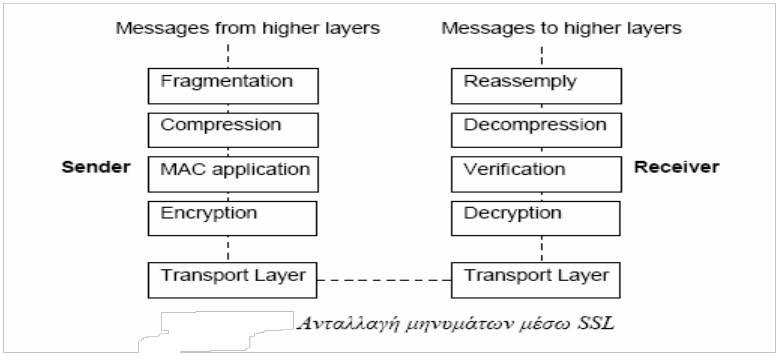
Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Right: 0,63 cm



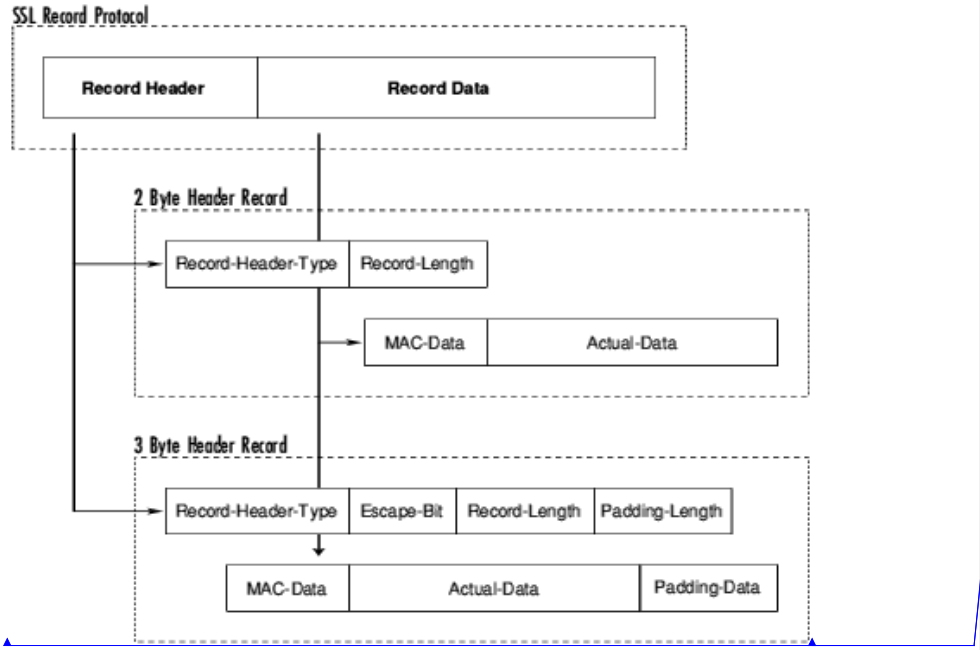
Ανταλλαγή μηνυμάτων μέσω SSL

5.1.2 Λειτουργία του SSL

Το SSL χωρίζεται σε δύο μέρη, το SSL Handshake Protocol (SSLHP) και το SSL Record Protocol (SSLRP). Το SSLHP διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του server και εάν ζητηθεί και του client. Το SSLRP συλλέγει τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει και αποκρυπτογραφεί τα παραλαμβανόμενα πακέτα.

A.SSL Record Protocol

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm



Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Ένα πακέτο SSL αποτελείται από δύο μέρη, την επικεφαλίδα και τα δεδομένα. Η επικεφαλίδα μπορεί να είναι είτε 3 bytes είτε 2 bytes, από τις οποίες περιπτώσεις η δεύτερη χρησιμοποιείται όταν τα δεδομένα χρειάζονται συμπλήρωμα (padding). Το πεδίο escape-bit στην περίπτωση των 3 bytes υπάρχει μόνο σε εκδόσεις μετά την δεύτερη του πρωτοκόλλου και προβλέπεται για ρύθμιση πληροφοριών out-of-band. Για την επικεφαλίδα των 2 bytes το μέγεθος του πακέτου είναι 32767 bytes, ενώ για την επικεφαλίδα των 3 bytes το μέγεθος είναι 16383 bytes.

Το κομμάτι των δεδομένων αποτελείται από ένα Message Authentication Code (MAC), τα πραγματικά δεδομένα και δεδομένα συμπλήρωσης, εάν χρειάζονται. Αυτό το κομμάτι είναι που κρυπτογραφείται κατά την μετάδοση. Τα συμπληρωματικά δεδομένα απαιτούνται όταν οι αλγόριθμοι κρυπτογράφησης εν χρήση είναι τύπου block ciphers και ο ρόλος τους είναι να συμπληρώνουν τα πραγματικά δεδομένα ώστε το μέγεθος τους είναι πολλαπλάσιου του μεγέθους που δέχεται σαν είσοδο ο block cipher. Εάν χρησιμοποιούνται stream ciphers τότε δεν απαιτείται συμπλήρωμα και μπορεί ~~αν~~ να χρησιμοποιηθεί η επικεφαλίδα των 2 bytes.

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

Το MAC είναι η digest ή hash value των secret-write key του αποστολέα του πακέτου, των πραγματικών δεδομένων, των συμπληρωματικών δεδομένων και ενός αριθμού ακολουθίας, στην σειρά που δίνονται.

Προβλέπεται και η συμπίεση των δεδομένων *(data compression)* με κατάλληλους μηχανισμούς που επιλέγονται κατά το handshake, ενώ δεν αποκλείεται να χρειαστεί και τεμαχισμός της πληροφορίας σε πολλά πακέτα *(fragmentation)*.

B. SSL Handshake Protocol

Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Το πρωτόκολλο SSL Handshake διαχωρίζεται σε δύο επιμέρους φάσεις: η πρώτη φάση αφορά την επιλογή των αλγόριθμων, την ανταλλαγή ενός master key και την πιστοποίηση της ταυτότητας του server. Η δεύτερη φάση διαχειρίζεται την πιστοποίηση της ταυτότητας του client (εάν ζητηθεί) και ολοκληρώνει την διαδικασία του handshaking. Όταν ~~το~~ ολοκληρωθούν και οι δύο φάσεις, το στάδιο του handshake τελειώνει και η μεταφορά μεταξύ των δύο άκρων αρχίζει. Όλα τα μηνύματα κατά την διάρκεια του handshaking και μετά στέλνονται σύμφωνα με το SSL Record Protocol.

Το πακέτο των αλγορίθμων κρυπτογράφησης *(Cipher Suite)* περιλαμβάνει την μέθοδο για την ανταλλαγή των κλειδιών, τον αλγόριθμο κρυπτογράφησης και τον μηχανισμό για την παραγωγή του MAC.

Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines

5.1.3 Αντοχή του SSL σε Γνωστές Επιθέσεις

Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial

Dictionary Attack

Αυτό το είδος της επίθεσης λειτουργεί όταν ένα μέρος του μη κρυπτογραφημένου κειμένου είναι στην κατοχή του ανέντιμων προσώπων. Το μέρος αυτό κρυπτογραφείται με χρήση κάθε πιθανού κλειδιού και έπειτα ερευνάται ολόκληρο το κρυπτογραφημένο μήνυμα μέχρι να βρεθεί κομμάτι του που να ταιριάζει με κάποιο από τα προϋπολογισμένα. Σε περίπτωση που η έρευνα έχει επιτυχία, τότε το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση ολόκληρου του μηνύματος έχει βρεθεί.

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

Το SSL δεν απειλείται από αυτήν την επίθεση αφού τα κλειδιά των αλγορίθμων του είναι πολύ μεγάλα των 128 bit. Ακόμα και οι αλγόριθμοι σε εξαγόμενα προϊόντα, υποστηρίζουν 128 bit κλειδιά και παρ' όλο που τα 88 bit αυτών μεταδίδονται ανασφάλιστα, ο υπολογισμός 2^{40} διαφορετικών ακολουθιών κάνει την επίθεση αδύνατο να επιτύχει.

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Brute Force Attack

Formatted: Line spacing: 1,5 lines

Η επίθεση αυτή πραγματοποιείται με την χρήση όλων των πιθανών κλειδιών για την αποκρυπτογράφηση των μηνυμάτων. Όσο πιο μεγάλα σε μήκος είναι τα χρησιμοποιούμενα κλειδιά, τόσο πιο πολλά είναι τα πιθανά κλειδιά. Τέτοια επίθεση σε αλγορίθμους που χρησιμοποιούν κλειδιά των 128 bits είναι τελείως ανούσια. Μόνο ο DES56 bit cipher είναι ευαίσθητος σε αυτήν την επίθεση, αλλά η χρήση του δεν συνιστάται.

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Replay Attack

Formatted: Line spacing: 1,5 lines

Όταν ένας τρίτος καταγράφει την ανταλλαγή μηνυμάτων μεταξύ client και server και προσπαθεί να ξανά χρησιμοποιήσει τα μηνύματα του client για να αποκτήσει πρόσβαση στον server, έχουμε την επίθεση replay attack. Όμως το SSL κάνει χρήση του connection-id, το οποίο παράγεται από τον server με τυχαίο τρόπο και διαφέρει για κάθε σύνδεση. Έτσι δεν είναι δυνατόν πότε να υπάρχουν δυο ίδια connection-id και το σύνολο των είδη χρησιμοποιημένων μηνυμάτων δεν γίνονται δεκτά από τον server. Το connection-id έχει μέγεθος 128 bit για πρόσθετη ασφάλεια.

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Man-In-The-Middle-Attack

Formatted: Line spacing: 1,5 lines

Η επίθεση Man-In-The-Middle συμβαίνει όταν ένας τρίτος είναι σε θέση να παρεμβάλλεται στην επικοινωνία μεταξύ του server και του client. Αφού επεξεργαστεί τα μηνύματα του client και τροποποιήσει όπως αυτός επιθυμεί, τα προωθεί στον server. Ομοίως πράττει για τα μηνύματα που προέρχονται από τον server. Δηλαδή, προσποιείται στον client ότι είναι ο server και αντίστροφα.

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Το SSL υποχρεώνει τον server να αποδεικνύει την ταυτότητα του με την χρήση έγκυρου πιστοποιητικού του οποίου η τροποποίηση είναι αδύνατον. Μην ξεχνάμε την δυνατότητα επικοινωνίας των κλειδιών υπογεγραμμένα.

Formatted: Right: 0,63 cm

5.1.4 Αδυναμίες του SSL

Brute Force Attack Εναντίον Αδύναμων Αλγορίθμων

Η μεγαλύτερη αδυναμία του πρωτοκόλλου είναι η ευαισθησία των αλγόριθμων που χρησιμοποιούν μικρά κλειδιά. Συγκεκριμένα, οι RC4-40, RC2-40 και DES-56 εισάγουν σοβαρά προβλήματα ασφαλείας και θα πρέπει να αποφεύγονται.

Renegotiation of Session Keys (μόνο στην 2 έκδοση)

Από την στιγμή που μία σύνδεση δημιουργηθεί, το ίδιο master key χρησιμοποιείται καθ' όλη την διάρκεια της. Όταν το SSL χρησιμοποιείται πάνω από μια μακρόχρονη σύνδεση (π.χ. μιας TELNET εφαρμογής), η αδυναμία αλλαγής του master key γίνεται επικίνδυνη. Η καλύτερη μέθοδος επίλυσης αυτού του προβλήματος είναι η επαναδιαπραγμάτευση του κλειδιού σε τακτά χρονικά διαστήματα, μειώνοντας έτσι την πιθανότητα μιας επιτυχής Brute Force Attack.

5.1.5 Χρήσεις του SSL

Η πιο κοινή του εφαρμογή είναι για την διασφάλιση HTTP επικοινωνιών μεταξύ του browser και του web server. Η ασφαλή έκδοση του HTTP χρησιμοποιεί URLs που ξεκινούν με "https" αντί του κανονικού "http" και διαφορετική πόρτα *(port)* που είναι η προκαθορισμένη στην 443. Ο browser αποθηκεύει τα ιδιωτικά κλειδιά του χρήστη και με κατάλληλο τρόπο υποδεικνύει την διενέργεια ασφαλών συνδέσεων.

Παρ' όλο που μπορεί κανείς να γράψει μια εφαρμογή του SSL ακολουθώντας τα *Internet drafts* και RFCs, είναι προτιμότερο να χρησιμοποιήσει μία από τις υπάρχοντες βιβλιοθήκες εργαλείων του SSL *(SSL toolkit Libraries)*. Τέτοιες βιβλιοθήκες περιέχουν ρουτίνες για κρυπτογράφηση, digestion, και διαχείριση πιστοποιητικών και διακρίνονται στις ακόλουθες:

- SSLRef
- SSLPlus
- SSLava
- SSLeay

Formatted: Font: (Default) Arial, 14 pt
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

5.2 S-HTTP (Secure- Http)

Formatted: Font: (Default) Arial, Not Highlight

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Το secure HTTP αναπτύχθηκε με σκοπό να παρέχει ασφαλείς μηχανισμούς επικοινωνίας μεταξύ HTTP πελατών και εξυπηρετητών και να τους δώσει τη δυνατότητα για ασφαλείς εμπορικές συναλλαγές. Είναι ένα ασφαλές προσανατολισμένο σε μηνύματα πρωτόκολλο, που σχεδιάστηκε για χρήση σε συνδυασμό με το απλό HTTP. Παρέχει ένα πλήθος από μηχανισμούς ασφαλείας και στους πελάτες και στους εξυπηρετητές, με συμμετρικές υπηρεσίες και δυνατότητες και για τους δύο, ενώ παράλληλα διατηρεί το μοντέλο επικοινωνίας και τα χαρακτηριστικά του HTTP.

Το S-HTTP παρέχει ασφαλείς από άκρο εις άκρο συναλλαγές, αντίθετα με τους μηχανισμούς εξουσιοδότησης στο HTTP, καθώς οι πελάτες ωθούνται στο να αρχίσουν ασφαλείς συναλλαγές χρησιμοποιώντας πληροφορίες στις επικεφαλίδες μηνυμάτων. Με το S-HTTP καμιά «ευαίσθητη» πληροφορία δεν είναι ανάγκη στο μεταδοθεί στο διαδίκτυο ανεξέλεγκτα. Επίσης το S-HTTP παρέχει πλήρη ευελιξία σε αλγόριθμους κρυπτογράφησης και παραμέτρους.

5.2.1 Το μοντέλο επεξεργασίας

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, Underline

Προετοιμασία μηνύματος

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Η δημιουργία ενός S-HTTP μηνύματος γίνεται από τον αποστολέα ενσωματώνοντας τις δικές του κρυπτογραφικές επιλογές με αυτές του παραλήπτη. Το αποτέλεσμα είναι μια λίστα από κρυπτογραφικές εμπλουτίσεις και κλειδιά, αρκεί να εφαρμοστούν. Για να γίνει αυτό, μπορεί να χρειαστεί η μεσολάβηση του χρήστη. Για παράδειγμα, μπορεί να παρέχονται πολλά κλειδιά για να υπογραφεί το μήνυμα. Με βάση αυτά τα δεδομένα, ο αποστολέας εφαρμόζει τις εμπλουτίσεις στο κείμενο του μηνύματος και δημιουργεί ένα S-HTTP μήνυμα.

Ανάκτηση μηνύματος

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Ο αποστολέας μπορεί ήδη να έχει δηλώσει ότι θα εκτελέσει κάποιες κρυπτογραφικές λειτουργίες πάνω στο μήνυμα. Για να ανακτήσει το S-HTTP μήνυμα , ο παραλήπτης πρέπει να διαβάσει ~~το~~ τις επικεφαλίδες για να

Formatted: Right: 0,63 cm

ανακαλύψει ποιοι κρυπτογραφικοί μετασχηματισμοί έγιναν στο μήνυμα, μετά να αφαιρέσει τους μετασχηματισμούς χρησιμοποιώντας κάποιο συνδυασμό των κλειδιών του αποστολέα και του παραλήπτη, ενώ παράλληλα θα σημειώνει ποιες εμπλουτίσεις έγιναν. Ο παραλήπτης μπορεί επίσης να επιλέξει να επικυρώσει ότι οι εφαρμοσμένες εμπλουτίσεις ταιριάζουν τόσο με τις εμπλουτίσεις που ο αποστολέας είπε ότι θα εφάρμοζε όσο και με αυτά που ο παραλήπτης ζήτησε, καθώς και με τις τρέχουσες κρυπτογραφικές προτιμήσεις, για να δει αν το S-HTTP μήνυμα μετασχηματίστηκε κατάλληλα. Αυτή η διαδικασία μπορεί να απαιτεί αλληλεπίδραση με το χρήστη για να επικυρώσει ότι οι εμπλουτίσεις είναι αποδεκτές στο χρήστη.

Διαπραγμάτευση

Formatted: Font: (Default) Arial

Για να προσφέρουν ευελιξία οι κρυπτογραφικές εμπλουτίσεις που χρησιμοποιούνται, ο πελάτης και ο εξυπηρετητής διαπραγματεύονται τις εμπλουτίσεις που ο καθένας προτίθεται να χρησιμοποιήσει, δεν προτίθεται να χρησιμοποιήσει, ή θα απαιτήσει να χρησιμοποιηθούν. Τα μπλοκ διαπραγμάτευσης αποτελούνται από τέσσερα μέρη: *ιδιότητα, τιμή*, *κατεύθυνση* και *ένταση*. Εάν οι πράκτορες δεν είναι ικανοί να ανακαλύψουν ένα κοινό σύνολο αλγορίθμων θα πρέπει να γίνουν οι κατάλληλες ενέργειες. Η συνεχής αίτηση μιας αρνούμενης επιλογής θεωρείται αναποτελεσματική και ακατάλληλη.

5.2~~2.5~~.2. Προστασία του μηνύματος

Formatted: Font: (Default) Arial, 14 pt, Underline

Η προστασία του μηνύματος μπορεί να παρέχεται σε τρεις άξονες:

Formatted: Font: (Default) Arial

- Υπογραφή
- Εξακρίβωση γνησιότητας
- Κρυπτογράφηση

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Πολλαπλοί μηχανισμοί διαχείρισης κλειδιού υποστηρίζοναι, συμπεριλαμβανομένου διαμοιραζόμενων μυστικών, με στυλ κωδικών, ανταλλαγή δημοσίου κλειδιού και διανομή εισιτηρίου (ticket) στον Κέρβερο. Συγκεκριμένα έχει γίνει πρόβλεψη για προκαθορισμένα συμμετρικά session κλειδιά με σκοπό να σταλούν εμπιστευτικά μηνύματα σε αυτούς που δεν έχουν ζευγάρι δημοσίου/ ιδιωτικού κλειδιού. Επιπρόσθετα ένας μηχανισμός

Formatted: Right: 0,63 cm

απόκρισης- πρόκλησης («nonce») παρέχεται για να επιτρέπει σε όσους θέλουν να επιβεβαιωθούν για το ότι η συναλλαγή έχει γίνει πρόσφατα.

Υπογραφή

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Αν εφαρμόζεται ο εμπλουτισμός της ηλεκτρονικής υπογραφής, είτε ένα κατάλληλο πιστοποιητικό μπορεί να προσαρτηθεί στο μήνυμα, είτε ο αποστολέας μπορεί να αναμένει από τον παραλήπτη να αποκτήσει το απαιτούμενο πιστοποιητικό ανεξάρτητα.

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Ανταλλαγή κλειδιών και κρυπτογράφηση

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Για την υποστήριξη της bulk κρυπτογράφησης, το S-HTTP ορίζει δύο μηχανισμούς μεταφοράς κλειδιού, έναν που να χρησιμοποιεί ανταλλαγή κρυπτογραφημένου κλειδιού και ένα άλλο με κλειδιά που είναι κανονισμένα εξωτερικά. Στην πρώτη περίπτωση, η παράμετρος τους συστήματος συμμετρικής κρυπτογράφησης περνιέται κρυπτογραφημένη με το δημόσιο κλειδί του παραλήπτη. Στην άλλη περίπτωση κρυπτογραφούμε το περιεχόμενο χρησιμοποιώντας ένα καθορισμένο session κλειδί με τις πληροφορίες αναγνώρισης κλειδιού να ορίζονται σε μια από τις γραμμές της επικεφαλίδας. Τα κλειδιά μπορούν ακόμα να εξαχθούν από τα εισιτήρια του Κέρβερου.

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Γνησιότητα μηνύματος και αποστολέα

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Το S-HTTP παρέχει ένα τρόπο για επικυρώνει την ακεραιότητα του μηνύματος και την εξακρίβωση γνησιότητας του αποστολέα για ένα μήνυμα μέσω του υπολογισμού ενός κωδικού εξακρίβωσης γνησιότητας μηνύματος (Message Authentication Code – MAC), που υπολογίζεται σαν ένα hash κλειδιού πάνω από το κείμενο, χρησιμοποιώντας ένα διαμοιρασμένο μυστικό το οποίο θα μπορούσε να έχει κανονιστεί με διάφορους τρόπους. Αυτή η τεχνική δεν απαιτεί ούτε την χρήση κρυπτογραφίας δημοσίου κλειδιού, ούτε κρυπτογράφησης.

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Ανανέωση

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Το πρωτόκολλο παρέχει ένα απλό μηχανισμό απόκρισης/ πρόκλησης, επιτρέποντας και στα δύο μέρη να επιβεβαιώσουν ότι οι μεταδόσεις έγιναν

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

πρόσφατα. Επιπρόσθετα, Η προστασία της ακεραιότητας που παρέχεται στις επικεφαλίδες του HTTP, αποδέχεται οι υλοποιήσεις να θεωρούν την επικεφαλίδα «Date:» ως ένα δείκτη ανανέωσης, όπου είναι δυνατό.

Nonces

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Τα Nonces είναι αδιαφανείς, προσωρινοί, προσανατολισμένοι-στη-συνοδό (session-oriented-identifiers, που μπορούν να χρησιμοποιηθούν για να παρέχουν μια ένδειξη ανανέωσης. Οι τιμές των Nonces είναι ένα θέμα τοπικό, αν και μπορεί απλά να είναι τυχαίοι αριθμοί που παράγονται από τον αποστολέα. Η τιμή παρέχεται απλά για να επιστραφεί από τον παραλήπτη.

Μορφή του μηνύματος

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Η σύνταξη του S-HTTP επίτηδες μιμείται την σύνταξη του HTTP σε μια προσπάθεια να διευκολύνει την ενσωμάτωση στα συστήματα που ήδη χρησιμοποιούν το HTTP. Επιπλέον, ορισμένες HTTP επικεφαλίδες γίνονται S-HTTP επικεφαλίδες, γιατί παρέχουν χρήσιμες λειτουργίες που έχουν προεκτάσεις στην ασφάλεια.

Ένα S-HTTP μήνυμα αποτελείται από μια γραμμή αίτησης ή κατάστασης (όπως και στο HTTP) Ακολουθούμενη από τις επικεφαλίδες που καθορίζονται στο RFC-822, ακολουθούμενα από ένα κρυμμένο κείμενο. Όταν ανακτάται το περιεχόμενο του κειμένου, μπορεί να είναι είτε ένα άλλο S-HTTP μήνυμα, είτε απλά δεδομένα.

Επικεφαλίδες

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Οι επικεφαλίδες που έχουν προστεθεί περιγράφονται στον παρακάτω πίνακα. Το S-HTTP παρέχει διάφορες δυνατότητες για το στάνταρ που θα ακολουθήσει την μορφή του μηνύματος από τους πελάτες και τους εξυπηρετητές, αλλά κυρίως χρησιμοποιούνται το PKCS-7 και το MOSS.

Formatted: Font: (Default) Arial, Greek

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

Ονομα παραμέτρου	Προαιρετική/ Απαιτούμενη	Ερμηνεία	Πιθανές Τιμές
Content-Privacy-domain	απαιτούμενη	Μορφή ενθυλακωμένου περιεχομένου	'MOSS','PKCS-7'
Content-Transfer-Encoding	προαιρετική	μέθοδος κωδικοποίησης	'BASE64', '8BIT' και όλες οι κωδικοποιήσεις του MOSS
Content-Type	απαιτούμενη	Τύπος	application/http application/shttp
Prearranged-Key-Info	προαιρετική	πληροφορία σχετική με το κλειδί που χρησιμοποιείται στην ενθυλάκωση του μηνύματος, για την ανταλλαγή κλειδιών	εσωτερικό (inband), εξωτερικό (outband), Κέρβερου
MAC-info	προαιρετική	ένα κωδικός (MAC) για την εξακρίβωση της γνησιότητας του μηνύματος	-

Οι επικεφαλίδες του μηνύματος στο S-HTTP

Ορισμένες HTTP ευκολίες και ιδιαίτερα εκείνες που αναφέρονται με το cashing και τους αντιπροσώπους (proxies), απαιτούν ειδική θεώρηση, όταν εφαρμόζεται S-HTTP επεξεργασία. Το S-HTTP παρέχει ειδική μεταχείριση για αυτά τα χαρακτηριστικά, αντιγράφοντας τις σχετικές HTTP επικεφαλίδες με S-HTTP σύνταξη. Οι επικεφαλίδες που έχουν εισαχθεί από το HTTP φαίνονται στον παρακάτω πίνακα.

Ονομα παραμέτρου	Ερμηνεία
Connection: Keep-Alive	Σχεδιασμένο για να επιτρέπει επίμονες συνδέσεις μεταξύ πελάτη/αντιπροσώπου και αντιπροσώπου/εξυπηρετητη
IF-Modified-Since	μπορεί να χρησιμοποιηθεί από τον αντιπρόσωπο για να δείξει ότι το έγγραφο μπορεί να βρίσκεται στην προσωρινή του μνήμη
Content-MD5	χρησιμοποιείται από τους εξυπηρετητές για να δίνουν τη δυνατότητα στους αντιπροσώπους να ανιχνεύουν αν έγιναν έγκυρες προσπελάσεις της ενδιάμεσης μνήμης.

Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

5.25.3 Το Πρωτόκολλο IPSec

Ο όρος IPSec (IP Security Protocol) αναφέρεται σε ένα σετ από μηχανισμούς που είναι σχεδιασμένοι να προστατεύουν την κίνηση στο επίπεδο IP. Οι υπηρεσίες που προσφέρει το πρωτόκολλο IPSec είναι η χωρίς σύνδεση (connectionless) ακεραιότητα (integrity) των δεδομένων, η εξακρίβωση γνησιότητας της προέλευσης δεδομένων, η προστασία απέναντι στις επαναλήψεις και η εμπιστευτικότητα. Αυτές οι υπηρεσίες εξασφαλίζονται στο επίπεδο IP γι' αυτό το λόγο προσφέρεται προστασία και στο επίπεδο IP και σε όλα τα επίπεδα που βρίσκονται πάνω από αυτό.

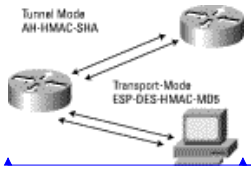
Το IPSec σχεδιάστηκε για να χρησιμοποιηθεί σε μεγάλο εύρος εφαρμογών. Όταν εφαρμοστεί σωστά, δεν επηρεάζει τα δίκτυα και τους υπολογιστές που δεν το στηρίζουν. Το IPSec είναι ανεξάρτητο από τους τρέχοντες κρυπτογραφικούς αλγορίθμους και μπορεί να χρησιμοποιήσει καινούργιους όταν γίνουν διαθέσιμοι. Το πρωτόκολλο IPSec δουλεύει και με τα δύο πρωτόκολλα IPV4 και IPV6. Συγκεκριμένα, είναι υποχρεωτικό μέρος του IPV6.

Συσχετισμοί Ασφάλειας – Security Association

Η IPSec παρέχει πολλές επιλογές για την υλοποίηση κρυπτογράφησης και πιστοποίησης ταυτότητας στο δίκτυο. Κάθε IPSec σύνδεση μπορεί να παρέχει είτε κρυπτογράφηση είτε ακεραιότητα και πιστοποίηση ταυτότητας δεδομένων ή και τα δυο. Όταν η υπηρεσία ασφάλειας καθοριστεί οι δυο επικοινωνούντες κόμβοι πρέπει να καθορίσουν ακριβώς ~~ποίουςποιους~~ αλγόριθμους θα χρησιμοποιήσουν (για παράδειγμα DES ή IDEA για κρυπτογράφηση και MD5 ή SHA για ακεραιότητα δεδομένων). Αφού αποφασίσουν για τους αλγόριθμους οι δυο συσκευές πρέπει να μοιράσουν κλειδιά σύνδεσης. Όπως μπορούμε να δούμε υπάρχει αρκετή πληροφορία προς παρακολούθηση. Η συσχέτιση ασφάλειας είναι μια μέθοδος που χρησιμοποιείται από την IPSec για την παρακολούθηση όλων των λεπτομερειών που αφορούν μια δεδομένη IPSec επικοινωνία. Μια συσχέτιση ασφάλειας είναι η σχέση μεταξύ δυο ή περισσοτέρων οντοτήτων που περιγράφει πως οι οντότητες θα χρησιμοποιήσουν τις υπηρεσίες ασφάλειας για να επικοινωνήσουν με ασφάλεια. Η νονμεκλατούρα μπερδεύει μερικές φορές διότι οι συσχετισμοί ασφάλειας χρησιμοποιούνται για πολλά

Formatted: Font: (Default) Arial, Greek, Not Highlight
Formatted: Bullets and Numbering
Formatted: Font: (Default) Arial, Greek, Not Highlight
Formatted: Font: (Default) Arial, Not Highlight
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

περισσότερα από ότι μόνο για την IPSec. Για παράδειγμα οι συσχετισμοί ασφάλειας IKE περιγράφουν τις παραμέτρους ασφάλειας μεταξύ δυο IKE συσκευών.



Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Οι συσχετισμοί ασφάλειας είναι μη κατευθυντικοί που σημαίνει ότι για κάθε ζεύγος επικοινωνούντων συστημάτων υπάρχουν τουλάχιστον δυο συνδέσεις ασφάλειας—μια από το A στο B και μια από το B στο A. Ο συσχετισμός ασφάλειας αναγνωρίζεται μοναδικά από έναν τυχαίως επιλεγμένο μοναδικό αριθμό ο οποίος λέγεται SPI (Security Parameter Index) και από την IP διεύθυνση του προορισμού. Όταν ένα σύστημα στέλνει ένα πακέτο το οποίο απαιτεί IPSec προστασία κοιτάει τον συσχετισμό ασφάλειας στη βάση δεδομένων του, εφαρμόζει τη συγκεκριμένη επεξεργασία και μετά εισάγει τον SPI από το συσχετισμό ασφάλειας στην IPSec επικεφαλίδα. Όταν το αντίστοιχο μηχάνημα IPSec λαμβάνει το πακέτο κοιτάει με τη σειρά του το συσχετισμό ασφάλειας βάσει της διεύθυνσης προορισμού και του SPI και μετά επεξεργάζεται το πακέτο όπως ορίζεται. Με λίγα λόγια ο συσχετισμός ασφάλειας είναι απλώς μια δήλωση της διαπραγματεύσιμης πολιτικής ασφάλειας μεταξύ δυο συσκευών

Πακέτα IPSec

Η IPSec ορίζει ένα νέο σετ επικεφαλίδων το οποίο προστίθεται στα IP διαγράμματα. Αυτές οι νέες επικεφαλίδες τοποθετούνται μετά την επικεφαλίδα IP και πριν το πρωτόκολλο επιπέδου 4 (τυπικά το TCP ή το UDP). Αυτές οι νέες επικεφαλίδες παρέχουν πληροφορίες για την ασφάλεια του φορτίου των IP πακέτων όπως αναλύεται παρακάτω:

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

- Επικεφαλίδα πιστοποίησης ταυτότητας (AH—Authentication Header)—αυτή η επικεφαλίδα όταν προστίθεται σε ένα IP διάγραμμα διασφαλίζει την ακεραιότητα και την ταυτότητα των δεδομένων. Δεν παρέχει ασφάλεια πιστότητας. Η επικεφαλίδα αυτή χρησιμοποιεί μια keyed-hash συνάρτηση αντί ψηφιακών υπογραφών διότι η τεχνολογία ψηφιακών υπογραφών είναι πολύ αργή και θα μείωνε την απόδοση του δικτύου.
- Φορτίο ασφαλείας ενθυλάκωσης (ESP—Encapsulating Security Payload)—αυτή η επικεφαλίδα όταν προστίθεται σε ένα IP διάγραμμα προστατεύει την ακεραιότητα και την ταυτότητα των δεδομένων. Αν η ESP χρησιμοποιείται για την επικύρωση της ακεραιότητας των δεδομένων δεν περιλαμβάνει τα αμετάβλητα πεδία της IP επικεφαλίδας.

Οι AH και οι ESP μπορούν να χρησιμοποιηθούν ανεξάρτητα ή μαζί, αν και για τις περισσότερες εφαρμογές μια από τις δυο είναι αρκετή. Και για τα δυο αυτά πρωτόκολλα οι IPSec δεν καθορίζει συγκεκριμένους αλγόριθμους που πρέπει να χρησιμοποιηθούν αλλά παρέχει ένα ανοικτό πλαίσιο για βιομηχανική υλοποίηση με παραγωγή ανεξάρτητων αλγορίθμων. Αρχικά οι περισσότερες υλοποιήσεις της IPSec θα περιλαμβάνουν υποστήριξη για το MD5 από την RSA Data Security ή για την SHA (Secure Hash Algorithm) όπως ορίζεται από την κυβέρνηση των Η. Π. Α. για την ακεραιότητα και την πιστοποίηση της ταυτότητας. Το DES (Data Encryption Standard) είναι προς το παρόν ο πιο κοινά προσφερόμενος αλγόριθμος κρυπτογράφησης αν και υπάρχουν και άλλοι όπως οι IDEA, Blowfish και RC4.

Το πρωτόκολλο ανταλλαγής κλειδιών

Το IKE (πρώην ISAKMP) που σημαίνει Internet Key Exchange είναι ένα πρωτόκολλο που σχεδιάστηκε για την υποστήριξη αυτόματων διαπραγματεύσεων των SA και αυτοματοποιημένης δημιουργίας και ανανέωσης κρυπτογραφικών κλειδιών.

Το πρωτόκολλο αυτό χρησιμοποιεί πολύπλοκες διαδικασίες κρυπτογράφησης και εξακρίβωσης γνησιότητας γιατί μέσω αυτού γίνονται

Formatted: Line spacing: 1,5 lines

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, Greek

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

ανταλλαγές πληροφοριών όπως κλειδιών, που χρειάζονται για την ασφάλεια των επικοινωνιών.

Οι μέθοδοι που χρησιμοποιεί το πρωτόκολλο IKE για εξακρίβωση γνησιότητας είναι οι παρακάτω:

1. Προ- διαμοιρασμένο κλειδί(Pre- Shared Key)
2. Ηλεκτρονικές υπογραφές(Digital Signatures- με Dss και RSA)
3. Κρυπτογράφηση δημοσίου κλειδιού(Public Key Encryption με RSA και revised RSA)

Η αποτελεσματικότητα μιας κρυπτογραφικής λύσης εξαρτάται περισσότερο από την ασφαλή μετάδοση του κλειδιού παρά από την επιλογή του αλγορίθμου. Έτσι, το IETF IPSec Working Group έχει περιγράψει μια σειρά από ιδιαίτερα ανθεκτικά πρωτόκολλα ανταλλαγής Oakley που χρησιμοποιούνται στο IKE. Αυτά χρησιμοποιούν μια προσέγγιση δύο φάσεων: Στην πρώτη φάση μετά από μια σειρά από διαπραγματεύσεις εγκαθίσταται ένα master κλειδί από το οποίο θα παράγονται όλα τα υπόλοιπα κρυπτογραφικά κλειδιά. Στην γενικότερη περίπτωση αυτό το κλειδί θα πραγματοποιήσει μια ασφαλή σύνδεση πάνω στην οποία θα μεταδίδονται τα μηνύματα του IKE. Η δεύτερη φάση είναι η ανταλλαγή των μηνυμάτων, αφού πρώτα γίνει η ασφαλής σύνδεση από την πρώτη φάση, για την παραγωγή κλειδιών με τα οποία θα εξασφαλιστεί η ασφαλής επικοινωνία των δεδομένων.

5.34 Pretty Good Privacy

Το σύστημα PGP είναι δημιουργία του P.Zimmermann και παρέχει υπηρεσίες

αυθεντικοποίησης και εμπιστευτικότητας για e-mail και εφαρμογές αποθήκευσης αρχείου

Δημόσια και Ιδιωτικά κλειδιά

Βασική προϋπόθεση για τη λειτουργία του PGP είναι ότι κάθε χρήστης πρέπει να

είναι κάτοχος ενός ιδιωτικού κλειδιού και του αντίγραφου του δημόσιου κλειδιού κάθε πιθανού συνομιλητή του. Το PGP διατηρεί έναν κατάλογο με τα δημόσια κλειδιά που οι χρήστες έχουν προμηθευτεί με τον έναν ή τον άλλο

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Indent: Left: 0 cm, First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Indent: Left: 0 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, Bold, Underline, Greek, Not Highlight

Formatted: Font: (Default) Arial, 14 pt, Underline, Not Highlight

Formatted: Font: (Default) Arial, 14 pt, Underline, Greek

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Greek

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

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.

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

- 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)

Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

- Το PGP κρυπτογραφεί το μήνυμα χρησιμοποιώντας τον αλγόριθμο IDEA με το κλειδί επικοινωνίας που δημιούργησε.
- Το PGP κρυπτογραφεί το κλειδί επικοινωνίας με τον αλγόριθμο RSA και το δημόσιο κλειδί του παραλήπτη και προσαρτά το αποτέλεσμα στο μήνυμα. Τέλος, ο προσδιοριστής του δημόσιου κλειδιού του παραλήπτη προσαρτάται επίσης στο κρυπτογραφημένο κλειδί επικοινωνίας.

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

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

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

Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

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 υπογεγραμμένο πιστοποιητικό 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~~ δημοσίου 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.

~~5.3~~5.5 S/MIME

Το S/MIME (Secure Multipurpose Internet Mail Extension) αποτελεί μια τεχνολογία ασφαλής μεταφοράς ηλεκτρονικών μηνυμάτων.

Το 1995, ορισμένοι πωλητές software δημιούργησαν S/MIME με σκοπό τη λύση του προβλήματος παραβίασης του e-mail από τρίτους.

Το S/MIME "χτίζει" την ασφάλεια του επάνω από το πρωτόκολλο MIME

Formatted: Line spacing: 1,5 lines, Bulleted + Level: 1 + Aligned at: 0,63 cm + Tab after: 1,27 cm + Indent at: 1,27 cm
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Bullets and Numbering
Formatted: Font: (Default) Arial, 14 pt, Underline, Greek, Not Highlight
Formatted: Font: (Default) Arial, 14 pt, Underline, Not Highlight
Formatted: Font: (Default) Arial, 14 pt, Underline, Greek
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

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

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

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

υπολογισμένο digest. Εαν τα δυο digest δεν είναι ίδια, τότε μπορεί να συμβαίνουν δύο τινα: ή το μήνυμα έχει ~~υπογραφηθεί~~υπογραφεί με ένα λανθασμένο ιδιωτικό κλειδί, είτε κάποιος έχει ~~παραλάξει~~παραλλάξει 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~~καθαυτό 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~~υιοθέτησης ενός μηχανισμού που θα προσδιορίζει με ασφάλεια τον αληθινό ιδιοκτήτη ενός δημόσιο κλειδιού. Η λύση σε αυτό το πρόβλημα παρέχεται με τα **ψηφιακά πιστοποιητικά** . Ένα πιστοποιητικό ουσιαστικά αντιστοιχεί ένα όνομα με ένα δημόσιο κλειδί. Το πιστοποιητικό ~~καθ'άυτό~~καθαυτό είναι υπογεγραμμένο από έναν τρίτο ανεξάρτητο

Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

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.~~

5.46 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 . Το Kerberos παρέχει προαιρετικά ακεραιότητα και εμπιστευτικότητα για δεδομένα που ~~μεραφέρονται~~μεταφέρονται 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.

Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, 14 pt, Underline, Not Highlight
Formatted: Font: (Default) Arial, 14 pt, Underline, Greek, Not Highlight
Formatted: Font: (Default) Arial, 14 pt, Underline, Not Highlight
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial, 14 pt, Bold, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

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~~εισιτηρίων" (**ticket granting service**) ώστε να υποστηρίζεται η συνακόλουθη αυθεντικοποίηση χωρίς επανα-πληκτρολόγηση του password του υποκειμένου, και μια διαφορετική προσέγγιση στη **σταυρωτή αυθεντικοποίηση** (cross-realm authentication), δηλαδή την αυθεντικοποίηση ενός υποκειμένου που είναι καταχωρημένο σε έναν διαφορετικό server αυθεντικοποίησης από ότι ο πιστοποιητής.

Κρυπτογράφηση στο Kerberos

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

Η κρυπτογράφηση στην παρούσα υλοποίηση του Kerberos χρησιμοποιεί το Data Encryption Standard (DES). Μια ιδιότητα του DES είναι ότι εαν ένα κρυπτογράφημα

Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

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~~ εισιτήρια στο Kerberos

Ο client και ο server δεν μοιράζονται εξαρχής ένα κλειδί κρυπτογράφησης. Όποτε

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

Το Kerberos εισητήριο είναι ένα πιστοποιητικό που εκδίδεται από έναν server

αυθεντικοποίησης, κρυπτογραφημένο με το κλειδί του server. Μεταξύ άλλων

πληροφοριών, το εισητήριο περιλαμβάνει το τυχαίο κλειδί επικοινωνίας που θα

χρησιμοποιηθεί για αυθεντικοποίηση του υποκειμένου στον πιστοποιητή, το όνομα του υποκειμένου (principal) για το οποίο εκδόθηκε το κλειδί επικοινωνίας, και ένα χρόνο διαρκείας (expiration time) μετά το πέρας του οποίου το κλειδί επικοινωνίας δεν ισχύει πλέον. Το ει~~σ~~ισιτήριο 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~~ εισιτήριο 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~~ εισιτήριο χωρίς να ανακαλυφθεί.

Αίτηση εφαρμογής και απάντηση

Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

Τα μηνύματα 3 και 4 στο παρακάτω σχήμα αναπαριστάνουν την αίτηση εφαρμογής

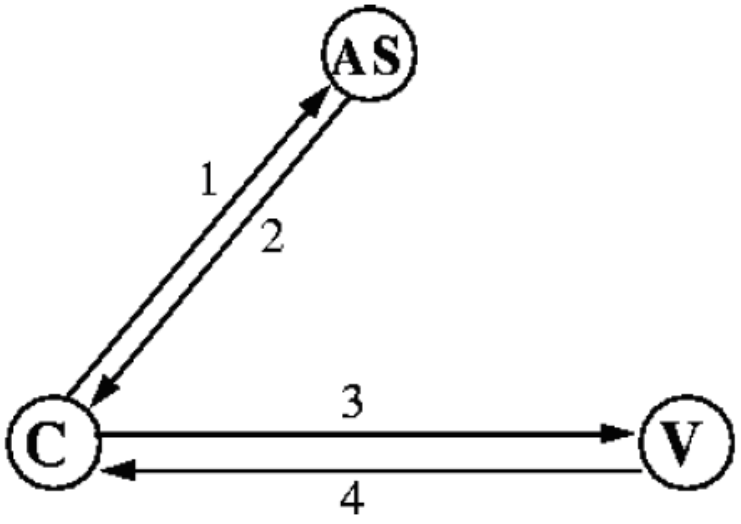
(application request) και την απάντηση (response), ίσως την πιο σημαντική ανταλλαγή μυνημάτων στο πρωτόκολλο Kerberos. Μέσω αυτών των μηνυμάτων ο client αποδεικνύει στον πιστοποιητή ότι γνωρίζει το κλειδί επικοινωνίας που είναι

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)

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

Βασικό πρωτόκολλο αυθεντικοποίησης στο kerberos (απλοποιημένο)

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

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 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 παραπάνω σχήματος (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 ~~αντιστοίχισηαντιστοίχηση~~ της αίτησης με την απάντηση.

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

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 ~~ενοίκιασηςενοικίασης εισητηρίωνεισιτηρίων~~” (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,

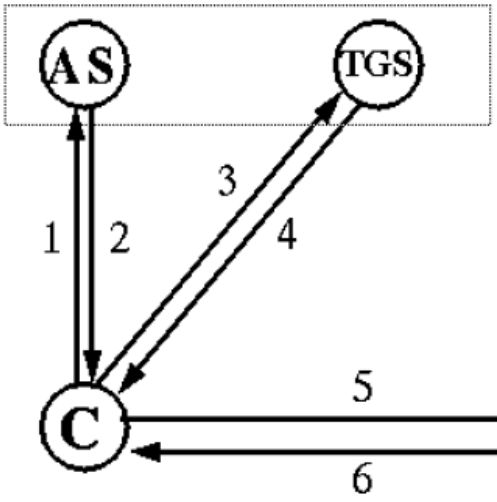
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

διατυπώνεται μια αίτηση αυθεντικοποίησης, και ο server αυθεντικοποίησης επιστρέφει ένα εισητήριο μαζί με ένα κλειδί επικοινωνίας για την “υπηρεσία ~~ενοίκιασης~~ενοικίασης ~~εισητηρίων~~εισιτηρίων”. 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~~εισιτηρίου (ticket granting exchange). Η επικοινωνία έκδοσης ~~εισητηρίου~~εισιτηρίου είναι παρόμοια με την επικοινωνία αυθεντικοποίησης (authentication exchange), με εξαίρεση το γεγονός ότι η αίτηση έκδοσης ~~εισητηρίου~~εισιτηρίου (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.

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek

Formatted: Right: 0,63 cm



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~~πρώτο-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.

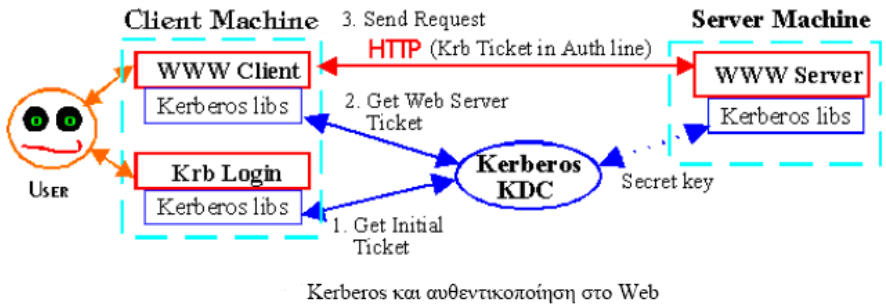
Kerberos και Web

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

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

Web . Έτσι, επιτυγχάνεται αμοιβαία αυθεντικοποίηση του server και του client, ο

server μπορεί να ασκήσει έλεγχο προσπέλασης με βάση την αυθεντικοποίηση του client, ενώ οι αιτήσεις και οι απαντήσεις του client και του server αντίστοιχα κρυπτογραφούνται για μεγαλύτερη ασφάλεια. Το παρακάτω σχήμα αναπαριστάνει τη διαδικασία.



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~~μεταβαίνει 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
```


Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

WWW-Authenticate: KerberosV4

3. Ο client παίρνει ένα εισητήριο για τον server, και ξανα-υποβάλλει την αίτηση,
~~εισαγάγονταςεισάγοντας~~ 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

5.~~5~~7 Linux - PAM (Pluggable Authentication Modules)

5.~~7~~5.1 Ορισμός - Σκοπός

Το Linux-PAM είναι σύνολο κοινών βιβλιοθηκών που επιτρέπουν στον τοπικό διαχειριστή του συστήματος να επιλέγει το τρόπο που οι διάφορες εφαρμογές πιστοποιούν τη γνησιότητα της ταυτότητας των χρηστών. Με άλλα

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, French (France)
Formatted: Font: (Default) Arial, French (France), Not Highlight
Formatted: Font: (Default) Arial, French (France)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

λόγια, χωρίς να είναι αναγκαίο να ξαναγραφτούν και να ξαναπεράσουν από τη διαδικασία του compilation οι συμβατές με το σύστημα PAM εφαρμογές, είναι δυνατόν να αλλάξει ο μηχανισμός με τον οποίο πραγματοποιούν την πιστοποίηση της ταυτότητας των χρηστών. Αυτό μπορεί να γίνει μέχρι του βαθμό της ολικής αναβάθμισης του συστήματος χωρίς να ενοχληθούν κατά οποιοδήποτε τρόπο οι διάφορες εφαρμογές.

Ιστορικά, μια εφαρμογή που απαιτούσε πιστοποίηση της ταυτότητας του χρήστη έπρεπε να περάσει από compilation για να μπορεί να χρησιμοποιήσει κάποιον συγκεκριμένο μηχανισμό πιστοποίησης της ταυτότητας του χρήστη. Για παράδειγμα στην περίπτωση των παραδοσιακών UNIX συστημάτων, η ταυτότητα του χρήστη πιστοποιείται με τη διαδικασία ελέγχου του κωδικού του χρήστη όταν αυτός θελήσει να μπει στο λογαριασμό του. Αυτός ο κωδικός αφού συμπληρωθεί στην αρχή του από "αλατάκι" δύο χαρακτήρων, κρυπτογραφείται με τη χρήση του crypt(3). Ο χρήστης πιστοποιείται έναντι του συστήματος εάν ο κρυπτογραφημένος κωδικός που εισήγαγε στο σύστημα είναι ίδιος με αυτόν που υπάρχει στο δεύτερο πεδίο της καταχώρησης του χρήστη στη βάση δεδομένων κωδικών του συστήματος - το αρχείο */etc/passwd*. Σε τέτοιου είδους συστήματα οι περισσότερες, αν όχι όλες, μορφές προνομίων παρέχονται από το σύστημα βάση αυτού του μοναδικού μηχανισμού πιστοποίησης. Τα προνόμια δίδονται με τη μορφή προσωπικών αριθμών *(user-id ή uid)* που ο κάθε χρήστης έχει και με τον οποίο εκπροσωπείται πλήρως στο σύστημα ή με τη μορφή αντίστοιχων αριθμών που χαρακτηρίζουν ολόκληρα σύνολα χρηστών *(group id ή gid)* στα οποία μπορεί να ανήκει κάποιος χρήστης και να απολαμβάνει και αυτός τα δικαιώματα που απορρέουν από την ύπαρξή του σε αυτό το σύνολο. Αυτά τα στοιχεία βρίσκονται κατά παράδοση στο αρχείο */etc/group*.

Ατυχώς, οι συνεχείς αυξήσεις της ταχύτητας των υπολογιστών και η πλατιά διάδοση των δικτυωμένων υπολογιστικών συστημάτων έχουν μετατρέψει τους άλλοτε ασφαλείς μηχανισμούς πιστοποίησης, σαν αυτόν, σε ευάλωτα σε επιθέσεις σχήματα. Οι διαπιστώσεις αυτές οδήγησαν στην ανάπτυξη νέων μηχανισμών πιστοποίησης της ταυτότητας του χρήστη.

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Ο σκοπός του Linux-PAM είναι ο διαχωρισμός της ανάπτυξης του λογισμικού χορήγησης προνομίων από την ανάπτυξη καταλλήλων μηχανισμών ασφάλειας. Αυτό επιτυγχάνεται με τη παροχή μιας βιβλιοθήκης λειτουργιών που μπορούν να χρησιμοποιηθούν από μια εφαρμογή για την πιστοποίηση της ταυτότητας του χρήστη. Αυτή η βιβλιοθήκη PAM ρυθμίζεται

Formatted: Right: 0,63 cm

τοπικά με τη βοήθεια ενός αρχείου συστήματος *(/etc/pam.conf)* ή με μια σειρά αρχείων ρυθμίσεων που βρίσκονται στο κατάλογο */etc/pam.d/* για να πιστοποιεί τους χρήστες μέσο των τοπικά διαθέσιμων modules (προγράμματα - πακέτα). Τα modules βρίσκονται συνήθως στο κατάλογο */usr/lib/security* και παίρνουν τη μορφή δυναμικά φορτώσιμων αρχείων αντικειμένων.

5.75.2 Επισκόπηση Λειτουργίας

Ας εξετάσουμε το παρακάτω παράδειγμα: Παίρνουμε μια εφαρμογή που χορηγεί κάποιου είδους υπηρεσία στους χρήστες. Το *login* είναι ένα τέτοιο πρόγραμμα. Το *login* κάνει δύο πράγματα: Πρώτον πιστοποιεί ότι ο χρήστης είναι αυτός που ισχυρίζεται και δεύτερον παρέχει την υπηρεσία που του ζητήθηκε και που στη περίπτωση του *login* είναι ένα command shell (κέλυφος εντολών) με τη ταυτότητα του χρήστη.

Παραδοσιακά, η παραπάνω διαδικασία επιτυγχάνεται ζητώντας από το χρήστη το password (κωδικό χρήστη) και πιστοποιώντας ότι αυτός είναι ο ίδιος με αυτόν που υπάρχει στο σύστημα. Με αυτό το τρόπο κάνει τη πιστοποίηση της ταυτότητας του χρήστη. Αυτή τη δουλειά ανατίθεται στο Linux-PAM. Από την οπτική γωνία του προγραμματιστή εφαρμογών (στη περίπτωσή μας του ατόμου που έφτιαξε το login πρόγραμμα), το Linux-PAM αναλαμβάνει το έργο της πιστοποίησης της ταυτότητας του χρήστη.

Η ευελιξία του συστήματος αυτού έγκειται στο γεγονός ότι ο διαχειριστής του έχει την ελευθερία να επιλέξει ακριβώς το τρόπο με τον οποίο η συγκεκριμένη εφαρμογή θα πιστοποιήσει το χρήστη. Ο διαχειριστής έχει την ευχέρεια να επιλέξει και να κάνει όποιες ρυθμίσεις θεωρεί ότι πρέπει να γίνουν για κάποιες ή και για όλες τις συμβατές με το σύστημα PAM εφαρμογές του συστήματός του. Αυτό σημαίνει ότι μπορεί να πιστοποιήσει κάνοντας χρήση ενός μηχανισμού απλής εμπιστοσύνης (pam_permit) μέχρι κάτι τόσο "παρανοϊκό" όσο ο συνδυασμός ελέγχου του αμφιβληστροειδούς χιτώνα, δείγματος φωνής και κωδικού μιας χρήσης!

Για να γίνει πιο σαφής η ευελιξία που προσφέρει αυτό το σύστημα ας θεωρήσουμε το παρακάτω παράδειγμα: ο διαχειριστής του δικτύου (γονιός) θέλει να βελτιώσει την ικανότητα των χρηστών του συστήματος (παιδιά). Μπορεί λοιπόν να ρυθμίσει το αγαπημένο τους παιχνίδι, το οποίο είναι φυσικά συμβατή εφαρμογή με PAM, να τα πιστοποιεί κάνοντας έναν απλό έλεγχο της ορθότητας ενός πολλαπλασιασμού τον οποίο το σύστημα θα θέτει σαν

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

απαίτηση για την είσοδο στο παιχνίδι. Είναι προφανές ότι αν το παιχνίδι αξίζει, τα παιδιά θα μάθουν την προπαίδειά τους. Όσο τα παιδιά μεγαλώνουν η πιστοποίηση μπορεί να αναβαθμίζεται σε κάτι άλλο – ίσως μια μεγάλη διαίρεση.

Το σύστημα Linux-PAM έρχεται σε επαφή με τέσσερις διαφορετικούς τύπους διαχειριστικής εργασίας. Αυτοί είναι: διαχείριση πιστοποίησης, διαχείριση λογαριασμών, διαχείριση σύνδεσης, διαχείριση κωδικών. Ο συσχετισμός του προτιμώμενου διαχειριστικού σχήματος με τη συμπεριφορά μιας εφαρμογής γίνεται με καταχωρήσεις στο σχετικό Linux-PAM αρχείο ρυθμίσεων. Οι λειτουργίες διαχείρισης εκτελούνται από τα modules που καθορίζονται στο αρχείο αυτό.

Η λειτουργία του συστήματος βήμα προς βήμα είναι η ακόλουθη: Μία εφαρμογή X αλληλεπιδρά με τη βιβλιοθήκη του Linux-PAM χωρίς να γνωρίζει κανένα από τα χαρακτηριστικά της ρυθμισμένης διαδικασίας πιστοποίησης. Η βιβλιοθήκη του Linux-PAM με τη σειρά της συμβουλεύεται τα περιεχόμενα του PAM αρχείου ρυθμίσεων και φορτώνει τα απαιτούμενα για την εφαρμογή modules. Αυτά ανήκουν σε μία από τις τέσσερις διαχειριστικές ομάδες και είναι τοποθετημένα με τη σειρά που εμφανίζονται στο αρχείο ρυθμίσεων. Όταν αυτά τα modules κληθούν από το Linux-PAM εκτελούν τις διάφορες εργασίες πιστοποίησης. Η οποιαδήποτε πληροφορία κειμένου που χρειάζεται να κινηθεί από και προς τον χρήστη, μπορεί να το κάνει χρησιμοποιώντας της conversation function.

5.75.3 Το Αρχείο Ρυθμίσεων του Linux-PAM

Το Linux-PAM έχει σχεδιαστεί από την αρχή για παροχή μέγιστης δυνατής ευελιξίας στον διαχειριστή του συστήματος όσον αφορά την ικανότητα χορήγησης προνομίων. Οι ρυθμίσεις γίνονται σε ένα από τα δύο διαφορετικά σχήματα. Στο αρχείο ρυθμίσεων ή στο κατάλογο ρυθμίσεων.

Στο αρχείο ρυθμίσεων /etc/pam.conf υπάρχουν γραμμές ρυθμίσεων που έχουν τη παρακάτω μορφή:

service-name module-type control-flag module-path arguments

- **Service-name** (όνομα υπηρεσίας) - Το όνομα της υπηρεσίας που σχετίζεται με αυτή τη καταχώρηση. Συνήθως το όνομα της υπηρεσίας

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

είναι το συμβατικό όνομα της συγκεκριμένης εφαρμογής. Για παράδειγμα, "ftpd", "rlogin", "su" κτλ. Δεν υπάρχει κανένα ειδικό service-name, το οποίο να καθορίζει έναν μηχανισμό πιστοποίησης. Έχει το όνομα "OTHER" και μπορεί να ορισθεί με κεφαλαία ή μικρά γράμματα. Πρέπει να παρατηρήσουμε ότι όταν υπάρχει κάποιο module το οποίο έχει ορισθεί για named υπηρεσία, το "OTHER" αγνοείται.

- **Module-type** (τύπος του module) - Ένας από τους τέσσερις τύπους (προς το παρόν) των module. Αναλυτικά:

1. **Auth**: Αυτός ο τύπος module παρέχει δύο δυνατότητες πιστοποίησης. Πρώτον, πιστοποιεί ότι ο χρήστης είναι αυτός που ισχυρίζεται δίνοντας οδηγίες στην εφαρμογή να ζητήσει από τη χρήστη το κωδικό του ή κάποιο άλλο μέσο πιστοποίησης της ταυτότητάς του. Δεύτερον, το module μπορεί να χορηγήσει ιδιότητα μέλους ενός group (ανεξάρτητα από το αρχείο /etc/groups) ή άλλα προνόμια μέσω δικών του αποκλειστικά διαδικασιών.
2. **Account**: Αυτό το module πραγματοποιεί διαχείριση λογαριασμών βασιζόμενο σε στοιχεία ξένα προς την πιστοποίηση του χρήστη. Χρησιμοποιείται για να επιτρέπει ή να απαγορεύει την πρόσβαση σε μια υπηρεσία κρίνοντας από την ώρα της μέρας, τους πόρους του συστήματος τη συγκεκριμένη στιγμή (μέγιστο αριθμό χρηστών) ή ακόμα και τη τοποθεσία του χρήστη που κάνει την αίτηση σύνδεσης (π.χ. ο root μπορεί να μπει στο σύστημα μόνο από τη κονσόλα).
3. **Session:** Πρωταρχικά, αυτό το module σχετίζεται με τις εργασίες που πρέπει να γίνουν πριν και μετά την παροχή συγκεκριμένης υπηρεσίας στους χρήστες. Τέτοιες για παράδειγμα εργασίες περιλαμβάνουν τη καταγραφή πληροφοριών που αφορούν το άνοιγμα και κλείσιμο κάποιων μετακινούμενων δεδομένων μεταξύ του χρήστη και του συστήματος, τη διαδικασία του mounting των καταλόγων και άλλες.
4. **Password:** Ο τελευταίος τύπος module χρειάζεται στην ανανέωση της πληροφορίας πιστοποίησης που σχετίζεται με το χρήστη. Γενικά υπάρχει ένα module για κάθε βασισμένο στο δίδυμο"αίτησης/απάντησης" τύπο module πιστοποίησης. Με άλλα λόγια κάθε δίδυμο έχει το δικό του σχήμα—σχέδιο πιστοποίησης.

- **Control-Flag**

Ένα από τα τέσσερα (προς το παρόν) τεκμήρια που καταδεικνύουν τη σοβαρότητα που σχετίζεται με το γεγονός της επιτυχίας ή αποτυχίας ενός module. Το Linux-PAM έχει προβλέψει για τη πυραμιδοποίηση των παρόμοιων modules, παρέχοντας μια μέθοδο κατά την οποία ο χρήστης έρχεται σε επαφή με παραπάνω από ένα μηχανισμό πιστοποίησης για κάθε υπηρεσία-εφαρμογή. Η εφαρμογή δεν ενημερώνεται για την επιτυχία ή την αποτυχία του κάθε module που υπάρχει στο αρχείο /etc/pam.conf. Αντί αυτού λαμβάνει μία περιληπτική απάντηση *επιτυχίας* ή *αποτυχίας* από τη βιβλιοθήκη του Linux-PAM. Η σειρά εκτελέσεως αυτών των εντολών είναι αυτή με την οποία με την οποία έχουν καταχωρηθεί στο αρχείο /etc/pam.conf.

Η πολιτική καθορισμού αυτών των απαντήσεων βασίζεται στα παρακάτω τρία control-flags:

1. **Required** (απαιτούμενο) - Αυτό δείχνει ότι είναι απαραίτητη η επιτυχία του module για την επιτυχία του τύπου του module (module-type). Πιθανή αποτυχία του module δεν θα εμφανιστεί με κανένα τρόπο στο χρήστη μέχρι να περατωθεί όλη η διαδικασία ελέγχου όλων των modules που απομένουν.
2. **Requisite** (απαιτούμενο) - Αυτό είναι παρόμοιο με το προηγούμενο με τη μόνη διαφορά ότι εάν ένα τέτοιο module επιστρέψει σήμα αποτυχίας τότε ο έλεγχος περνάει αμέσως στην εφαρμογή. Το απαντητικό σήμα είναι αυτό που προκύπτει από τη πρώτη αποτυχία ενός *required* ή *requiresite* flag που θα αποτύχει. Αυτό το flag μπορεί να χρησιμοποιηθεί για την προστασία απέναντι στη πιθανότητα ένας χρήστης να στείλει το κωδικό του μέσα από ένα μη ασφαλές μέσο. Είναι πιθανό μια τέτοια συμπεριφορά να πληροφορήσει κάποιον επιτιθέμενο τους λογαριασμούς του συστήματος αλλά αυτή η πιθανότητα πρέπει να ζυγιστεί με την πιθανότητα της έκθεσης ευαίσθητων κωδικών σε ένα εχθρικό περιβάλλον.
3. **Sufficient** (ικανό) - Η επιτυχία αυτού του module θεωρείται ικανή από τη βιβλιοθήκη Linux-PAM για την επιτυχία του module-type. Στη περίπτωση που κανένα προηγούμενο required module δεν έχει αποτύχει, σταματάνε να ελέγχονται όλα τα παρόμοια με αυτό που έχουν στοιβαχτεί από τη βιβλιοθήκη. (Παρατηρούμε ότι σε αυτή τη

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

περίπτωση κανένα μεταγενέστερο required module δεν ελέγχεται). Πιθανή αποτυχία αυτού του module δεν θεωρείται μοιραία για την ικανοποίηση της εφαρμογής αυτού του module-type.

4. **Optional** (προαιρετικό) - Όπως και το όνομά του υπονοεί αυτό το control flag χαρακτηρίζει το module σαν όχι κρίσιμο για την επιτυχία ή αποτυχία της αίτησης του χρήστη για παροχή συγκεκριμένης υπηρεσίας. Ωστόσο, στην απουσία οποιονδήποτε επιτυχιών προηγουμένων ή μεταγενέστερων στοιβαγμένων modules η φύση της απάντησης στην εφαρμογή θα καθοριστεί από αυτό το module.

- **Module Path**

  Το path (μονοπάτι) του δυναμικού φορτιζόμενου αρχείου αντικειμένου, δηλαδή το ίδιο το module. Εάν ο πρώτος χαρακτήρας του path είναι "/", τότε θεωρείται πλήρες το path. Εάν δεν είναι αυτή η περίπτωση το χορηγηθέν path για το module θεωρείται ότι αναφέρεται στο παρακάτω path:/usr/lib/security.

- **Args**

  Τα args είναι μια λίστα τεκμηρίων που ενσωματώνονται στο module την ώρα που αυτό ελέγχεται όπως και τα arguments μιας τυπικής Linux εντολής κελύφους. Γενικά τα args είναι προαιρετικά αλλά και συγκεκριμένα για κάθε module. Μη έγκυρα args αγνοούνται από τα modules αλλά καταγράφεται το λάθος υποχρεωτικά στο syslog.

5.57.4 Ρύθμιση Βασισμένη σε Κατάλογο

Από την έκδοση 0.56 παρέχεται ένας πιο ευέλικτος τρόπος ρύθμισης του libpam. Αυτός ο τρόπος συνίσταται στη ρύθμιση των περιεχομένων του /etc/pam.d/ καταλόγου. Στη περίπτωση αυτή ο κατάλογος γεμίζει με αρχεία το καθένα από τα οποία έχει όνομα ίδιο με το όνομα μιας υπηρεσίας - είναι το προσωπικό αρχείο ρυθμίσεων της υπηρεσίας αυτής. Η ύπαρξη του κατάλογου /etc/pam.d/ σημαίνει ότι αγνοείται πλήρως το περιεχόμενο του αρχείου /etc/pam.conf . Το συντακτικό αυτού του αρχείου είναι παρόμοιο με αυτό του /etc/pam.conf αρχείου και οι καταχωρήσεις έχουν τη μορφή:

module-type control-flag module-path arguments

Η μόνη διαφορά, όπως παρατηρούμε, από το συντακτικό του αρχείου ρυθμίσεων είναι η έλλειψη του service-name, αυτό όμως συμπίπτει με το όνομα του αρχείου.

Αυτή η μέθοδος ρυθμίσεων έχει πολλά πλεονεκτήματα σε σχέση με τη προηγούμενη. Μερικά από αυτά είναι:

- Μικρότερη πιθανότητα κακής ρύθμισης της εφαρμογής. Υπάρχει ένα πεδίο λιγότερο που προσφέρεται για τυπογραφικά λάθη.
- Πιο εύκολο στη διατήρηση. Μία εφαρμογή μπορεί να επαναρυθμιστεί χωρίς το κίνδυνο να επηρεάσει άλλες εφαρμογές στο σύστημα.
- Είναι δυνατόν να διασυνδεθούν (to softlink) αρχεία ρυθμίσεων διαφορετικών υπηρεσιών σε ένα και μόνο αρχείο. Αυτό κάνει πιο εύκολη τη διατήρηση σταθερής πολιτικής πρόσβασής ανεξάρτητα των εφαρμογών.
- Δίνει τη δυνατότητα γρηγορότερης ανάλυσης των αρχείων. Μόνο οι σχετικές καταχωρήσεις αναλύονται όταν η υπηρεσία απασχολείται με τα modules της.
- Είναι δυνατό να περιοριστεί η πρόσβαση διαβάσματος (read access) σε μεμονωμένα Linux-PAM αρχεία ρυθμίσεων χρησιμοποιώντας τη προστασία αρχείων του συστήματος αρχείων (filesystem).

5.75.5 Οδηγός Αναφοράς Διαθέσιμων Modules

Παρακάτω παρατίθεται μια λίστα με τα διαθέσιμα από το Linux-PAM modules:

- Chroot
- Cracklib pluggable password strength-checker
- The looking-out module
- Set/unset environment variables
- Filter
- Anonymous access
- Group access
- Kerberos 4
- Resource limits
- List-file
- Mail

Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

- No-login
- Promiscuous
- Password-Database
- RADIUS
- Rhosts
- Root access
- Securetty
- Time control
- Warning logger
- Wheel

5.~~68~~ Το πρωτόκολλο SET

5.~~68~~.1 Γενικά χαρακτηριστικά

Το πρωτόκολλο Secure Electronic Transactions χρησιμοποιείται σήμερα ως

standard από πολλές τράπεζες και εταιρίες πιστωτικών καρτών, ως ο μόνος τρόπος για ασφαλές ηλεκτρονικό εμπόριο και προστασία των αριθμών πιστωτικών καρτών από κλοπή και εκμετάλλευση. Το πρωτόκολλο σχεδιάστηκε ώστε να επιτρέπει στους χρήστες του Internet να αγοράζουν προϊόντα από έμπορους στο Web, κατά τέτοιον τρόπο ώστε ο έμπορος να μη βλέπει ποτέ τον κωδικό πιστωτικής κάρτας του πελάτη, και η τράπεζα να μη μαθαίνει ποτέ τί παρήγγειλε ο πελάτης από τον έμπορο. Το SET λοιπόν, ενδυναμώνει το ηλεκτρονικό εμπόριο εξασφαλίζοντας την ιδιωτικότητα των συναλλαγών (θεωρητικά).

Προκειμένου να χρησιμοποιήσουν το SET, οι πελάτες πρέπει να πληκτρολογήσουν τους κωδικούς των πιστωτικών τους καρτών σε ένα ειδικό "wallet"

πρόγραμμα στους υπολογιστές τους. Όταν ένας πελάτης επιθυμεί να αγοράσει ένα

προϊόν, επιλέγει ένα link ή button, και ο έμπορος (ο server) του στέλνει ένα ειδικό αρχείο με συγκεκριμένο τύπο MIME, που περιγράφει το προϊόν.

- Ο υπολογιστής του πελάτη παίρνει το αρχείο, και υπολογίζει τη hash τιμή του. Ο υπολογιστής του πελάτη κρυπτογραφεί επίσης και τις

Formatted: Font: (Default) Arial, Bold, Greek, Not Highlight
Formatted: Font: (Default) Arial, Not Highlight
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines, Bulleted + Level: 1 + Aligned at: 0,63 cm + Tab after: 1,27 cm + Indent at: 1,27 cm
Formatted: Right: 0,63 cm

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.

5.68.2 Συστατικά Στοιχεία του SET

Τα συστατικά στοιχεία του συστήματος SET είναι τέσσερα και είναι τα παρακάτω:

- **Cardholder Wallet (Πορτοφόλι Χρήστη Κάρτας)**

  Είναι ένα προϊόν που χρησιμοποιεί ο καταναλωτής που βρίσκεται on-line και που επιτρέπει την πραγματοποίηση ασφαλών συναλλαγών σε ένα δίκτυο. Το Wallet πρέπει να δημιουργεί μηνύματα που τα αντιλαμβάνονται τα άλλα τρία προϊόντα που απαρτίζουν το SET (Merchant, Payment Gateway, Certificate Authority).

Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines, Bulleted + Level: 1 + Aligned at: 0,63 cm + Tab after: 1,27 cm + Indent at: 1,27 cm
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines, Bulleted + Level: 1 + Aligned at: 0,63 cm + Tab after: 1,27 cm + Indent at: 1,27 cm
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

- **Merchant Server (Server - Έμπορος)**

  Είναι ένα προϊόν το οποίο τρέχει κάποιος on-line έμπορος για την επεξεργασία των στοιχείων των συναλλαγών και τη διεκπεραίωσή τους. Επικοινωνεί και αυτό με τα άλλα τρία μέρη του SET.

- **Payment Gateway (Πύλη Πληρωμών)**

  Είναι το προϊόν που τρέχει κάποιος τρίτος ο οποίος και επεξεργάζεται την πιστοποίηση των εμπόρων και των συναλλαγών (συμπεριλαμβανομένων οδηγιών πληρωμών από κατόχους καρτών). Επιπλέον αλληλεπιδρά και με ιδιωτικά εμπορικά δίκτυα.

- **Certificate Authority (Υπηρεσία Πιστοποιητικών)**

  Είναι το τελευταίο από τα συστατικά στοιχεία του SET το οποίο τρέχει μια αρμόδια υπηρεσία έκδοσης και πιστοποίησης ψηφιακών πιστοποιητικών για το σκοπό αυτό και όποτε ζητείται από τα Wallet, Merchant και Payment Gateway πάνω από δημόσια ή ιδιωτικά δίκτυα.

Το SET σαν πρωτόκολλο έχει ήδη υιοθετηθεί από τράπεζες και οικονομικούς οργανισμούς παγκοσμίως. Παρακάτω παρατίθενται σε μορφή πίνακα τα χαρακτηριστικά του και μια σύντομη αναφορά στο τι ακριβώς σημαίνουν.

Ανοικτές Προδιαγραφές	Το SET είναι πρωτόκολλο ανοικτών προδιαγραφών που έχει επιλεγεί παγκοσμίως από μεγάλα χρηματοπιστωτικά ιδρύματα για συναλλαγές με πιστωτικές κάρτες στο Internet
Βιομηχανική Υποστήριξη	Το SET έχει την υποστήριξη των κυριότερων μελών της βιομηχανίας πιστωτικών καρτών όπως οι Visa,

	MasterCard, American Express και JCB
Ανεξαρτησία Πλατφόρμας	Το SET έχει σχεδιαστεί να είναι ανεξάρτητο από οποιαδήποτε συγκεκριμένη πλατφόρμα
Διαλειτουργικότητα	Το SET είναι το μόνο πρωτόκολλο ηλεκτρονικού εμπορίου που σχεδιάστηκε για συνεργασία με πολλαπλά προγράμματα που προέρχονται από διαφορετικούς κατασκευαστές
Επέκταση της Υπάρχουσας Υποδομής	Το SET επεκτείνει την υπάρχουσα υποδομή πιστωτικών καρτών στο Internet
Δυνατή Ασφάλεια	Το SET χρησιμοποιεί τεχνολογία κρυπτογράφησης για να προστατεύσει ευαίσθητες πληροφορίες από τα αδιάκριτα βλέμματα τρίτων
Πιστοποίηση	Η τεχνολογία SET πιστοποιεί όλα τα εμπλεκόμενα, σε μια συναλλαγή, μέρη κάνοντας χρήση ψηφιακών πιστοποιητικών
Περιβάλλον Εμπιστοσύνης	Το SET χρησιμοποιεί ένα ιεραρχικό σχήμα πέντε επιπέδων πιστοποίησης της εγκυρότητας, διασφαλίζοντας ένα περιβάλλον εμπιστοσύνης για το ηλεκτρονικό εμπόριο
Λύσεις End-to-End	Το SET πιστοποιεί και εγκρίνει όλα τα εμπλεκόμενα μέρη

Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

5.~~7~~9 PIX Firewall & Cisco IOS Firewall

5.~~7~~9.1 Εισαγωγή

Ο PIX Firewall είναι ένα πρωτοποριακό όργανο ασφάλειας που προσφέρει την υψηλότερη απόδοση ανάμεσα σε όλα τα συστήματα της βιομηχανίας (σύμφωνα με τα KeyLabs). Κάνοντας χρήση proxy συστημάτων πιστοποιεί τους χρήστες έναντι των RADIUS ή TACACS+ σε πολύ υψηλές ταχύτητες. Το λογισμικό της NetPartner, WebSENSE το οποίο διαχειρίζεται την πρόσβαση στο internet έχει ενσωματωθεί στο PIX Firewall με σκοπό να μπλοκάρει την εκτός ορίων πρόσβαση σε αμφισβητήσιμο ή αντιπαραγωγικό περιεχόμενο. Ο PIX Firewall κάνει χρήση hardware για κρυπτογράφηση και επιτάχυνση και υποστηρίζει το standard IPSec. Έτσι ο PIX Firewall καθίσταται η ιδανική λύση για το ηλεκτρονικό εμπόριο που αναπτύσσεται στο internet και για τη δημιουργία υψηλών αποδόσεων Virtual Private Network—VPNs δικτύων.

Ο Cisco IOS Firewall είναι μία συγκεκριμένη λύση ασφάλειας που "κάθεται" πάνω στο πιο διαδεδομένο λειτουργικό σύστημα δικτύων, το Cisco Internetwork Operating System (Cisco IOS Software). Ο Cisco IOS Firewall αυξάνει τις υπάρχουσες δυνατότητες του Cisco IOS λογισμικού όπως τη πιστοποίηση και τη κρυπτογράφηση με τελευταίας λέξης τεχνολογία. Αυτή η δήλωση περιλαμβάνει σταθερό φιλτράρισμα σε επίπεδο εφαρμογής, άμυνα έναντι δικτυακών επιθέσεων όπως "πλημμύρα" sync, ανίχνευση πορτών, διείσδυση πακέτων, μπλοκάρισμα της Java και VPNs βασισμένα στο Cisco IOS IPSec. Ο Cisco IOS Firewall παρέχει δυνατότητα δρομολόγησης πολλαπλών πρωτοκόλλων διότι τρέχει σε Cisco IOS βασισμένους δρομολογητές και κατά συνέπεια απολαμβάνει όλα εκείνα τα χαρακτηριστικά που αυτοί μπορούν και προσφέρουν.

5.~~9~~7.2 Σχηματική Αναπαράσταση του Τρόπου Ασφάλισης των Δικτύων από τους PIX και Cisco IOS Firewalls

Formatted: Font: (Default) Arial, Underline, Not Highlight

Formatted: Font: (Default) Arial, Underline

Formatted: Font: (Default) Arial, Underline

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

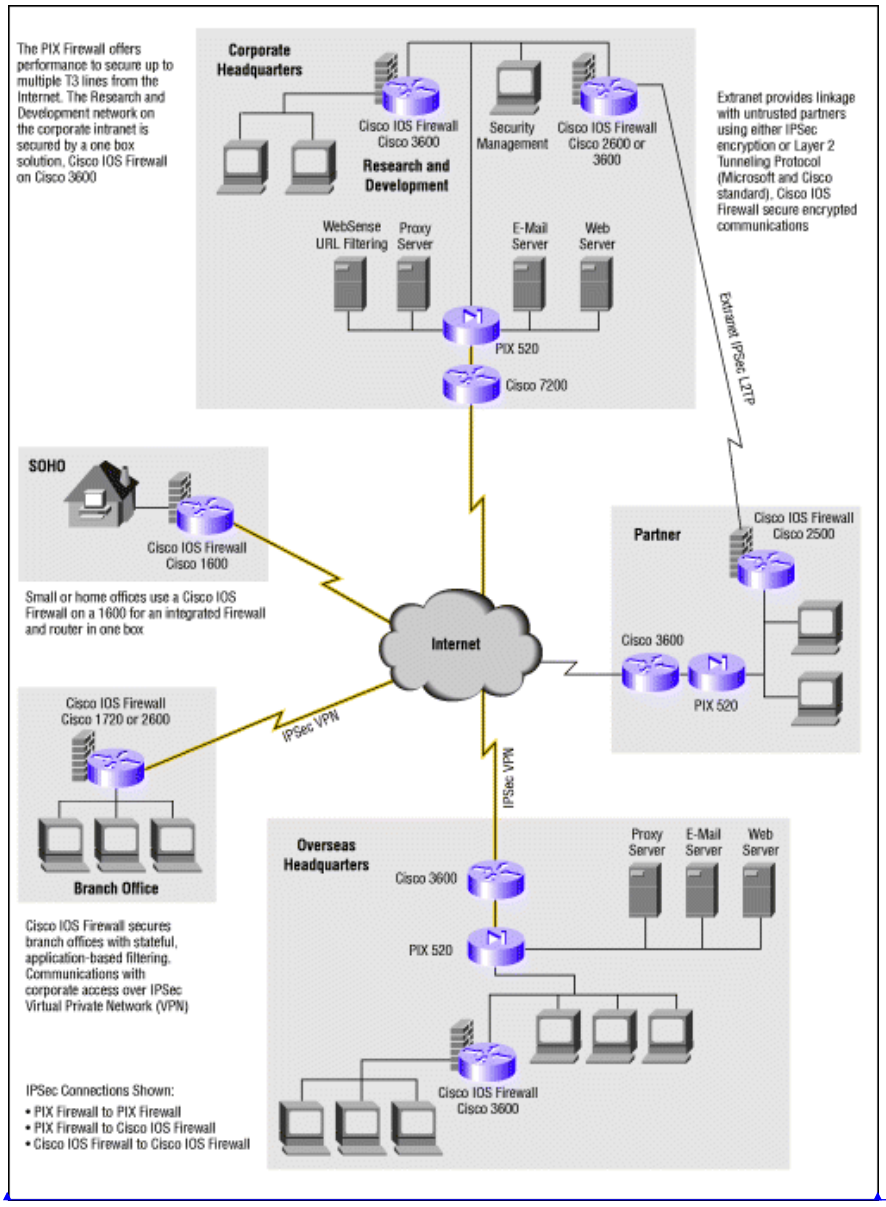
Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, 14 pt, Greek

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Right: 0,63 cm



5.97.3 Δυνατότητες Αιχμής των PIX και Cisco IOS Firewalls

Τόσο η σειρά Cisco PIX Firewall όσο και η Cisco IOS Firewall εφαρμόζουν τεχνολογία αιχμής. Ο πίνακας 1 δίνει μία άποψη των κοινών εξελιγμένων χαρακτηριστικών και των δύο Firewall.

Πίνακας 1

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

Χαρακτηριστικά και Πλεονεκτήματα των

PIX και Cisco IOS Firewalls

Χαρακτηριστικά	Πλεονεκτήματα
Ισχυρό φιλτράρισμα πακέτων	Παρέχει ισχυρή ασφάλεια ερευνώντας σχολαστικά τα πακέτα δεδομένων και διατηρώντας κρίσιμες διευθύνσεις και αριθμούς πορτών σε πίνακα
IPSec Virtual Private Network	Μειώνει το επικοινωνιακό κόστος δίνοντας τη δυνατότητα σε απομακρυσμένους χρήστες να έχουν πρόσβαση μέσω internet
Πιστοποίηση ταυτότητας και Έγκριση Dial-in Επικοινωνιών	Πιστοποίηση των χρηστών έναντι βιομηχανικών standards όπως τα TACACS+ και RADIUS
Μετάφραση Δικτυακών Διευθύνσεων (NAT)	Κρύβει το εσωτερικό δίκτυο από το εξωτερικό για αυξημένη ασφάλεια
Φιλτράρισμα Περιεχομένων	Μπλοκάρει εχθρικά Java applets
Διαχείριση	Διαχείριση βασισμένη σε GUI που επιτρέπει τον κεντρικό έλεγχο των firewall και των πολιτικών ασφάλειας. Εργαλεία δημιουργίας αναφορών, στατιστικών στοιχείων και άλλων λειτουργιών παρακολούθησης
Πλεονασμός/Μετάπτωση	Σε περίπτωση πτώσης όλη η κίνηση δρομολογείται σε κάποια backup μονάδα
Ασφάλεια για Servers που τρέχουν Δημόσιες Εφαρμογές	Τρίτο interface για το PIX ή το Cisco IOS που παρέχει απομονωμένο

Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

	δίκτυο για δημόσια προσβάσιμους servers όπως Web, e-mail, FTP ή DNS
Εκτεταμένη Υποστήριξη Multimedia περιλαμβανομένων των:Microsoft NetShow, White Pine CU-SeeMe, RealNetworks, RealAudio and RealVideo, Xing StreamWorks, VDONet VDO Live, Vxtreme WebTheatre, VocalTech Internet Phone, Microsoft NetMeeting, Intel Internet VideoPhone, White Pine Meeting Point	Οι πιο πρόσφατες media εφαρμογές διαθέσιμες χωρίς την ανάγκη ρυθμίσεων κάθε workstation
Ανίχνευση Εισβολής και Παρεμπόδισή ~~της~~ της	Ανίχνευση και παρεμπόδιση επίθεσης denial-of-service και άμυνα απέναντι πλημμύρας sync, ανίχνευση πορτών, διείσδυση πακέτων
Κρυπτογράφηση	Κρυπτογραφεί δεδομένα για ιδιωτικές επικοινωνίες πάνω από ανασφαλή δίκτυα

Αν και τα δύο συστήματα είναι πολύ καλά, έχουν κάποιες διαφορές που τα κάνουν καταλληλότερα ή όχι για συγκεκριμένες εργασίες.

5.~~9~~7.4 Οδηγός Προτίμησης

Πότε Διαλέγουμε τον PIX Firewall

Απαιτήσεις Πελάτη	Πλεονέκτημα του PIX
Αφιερωμένη Συσκευή στην Ασφάλεια	Προσφέρει αφιερωμένα όργανα με ειδικό hardware και software για βέλτιστη προστασία από το firewall

Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

Πολύ Γρήγορη Κρυπτογράφηση και VPNs	Hardware-Επιταχυνόμενη κρυπτογράφηση 56-bit DES και 3DES, IPSec VPNs
Υψηλή Internet Δραστηριότητα	Παρέχει δυνατότητα 65. 536 ταυτόχρονων συνδέσεων και περίπου 170 Mbps κίνησης κάνοντάς το ιδανικό για multimedia πρωτόκολλα, κρυπτογράφηση και μεγάλους αριθμούς χρηστών
Πιστοποίηση και Έγκριση	Ο PIX Firewall χρησιμοποιεί τα RADIUS και TACACS+ για πιστοποίηση
Φιλτράρισμα URL	Φιλτράρει URLs σε συνδυασμό με το WebSENSE της NetPartner

Πότε Διαλέγουμε τον Cisco IOS Firewall

Απαιτήσεις Πελάτη	Πλεονέκτημα του Cisco IOS
Λύση πακέτο όσον αφορά το συνδυασμό δυνατής ασφάλειας και δρομολόγησης πολλαπλών πρωτοκόλλων	Προσφέρει εξελιγμένα χαρακτηριστικά firewall όπως φιλτράρισμα πακέτων, μπλοκάρισμα της Java, κρυπτογράφηση, πιστοποίηση, IPSec VPNs και δρομολόγηση πολλαπλών πρωτοκόλλων—όλα σε ένα πακέτο
Ανταποδοτική προστασία τόσο των intranets όσο και των extranets	Είναι πιο οικονομικό για sites που δεν έχουν αυξημένες απαιτήσεις και άρα ανάγκη του PIX σαν προϊόν εξειδικευμένο
Ικανότητα λειτουργίας σε διαφορετικά Cisco IOS περιβάλλοντα με	Δυνατότητα ρύθμισης της απόδοσης στο επίπεδο που επιλέγουμε σε όλο

διαφορετικές απαιτήσεις απόδοσης	το φάσμα μοντέλων.
Εύκολη εκπαίδευση και συντήρηση	Οι εταιρίες που χρησιμοποιούν ήδη το Cisco IOS βρίσκουν το Cisco IOS Firewall πολύ γνώριμο στο στήσιμο και τη λειτουργία του
Επιπλέον ασφάλεια ενσωματωμένη στη δικτυακή υποδομή	Για τις εταιρίες με αυξημένες ανάγκες ασφάλειας μπορεί να εφαρμοστεί σε διάφορα σημεία της δικτυακής τους υποδομής

Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines

5.108 Virtual Private Networks (Ιδιωτικά Εικονικά Δίκτυα)

Formatted: Font: (Default) Arial, Not Highlight
Formatted: Font: (Default) Arial

Η μεταφορά μέσω του Internet εμπιστευτικής πληροφορίας, με έναν αξιόπιστο

Formatted: Font: (Default) Arial, Greek

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

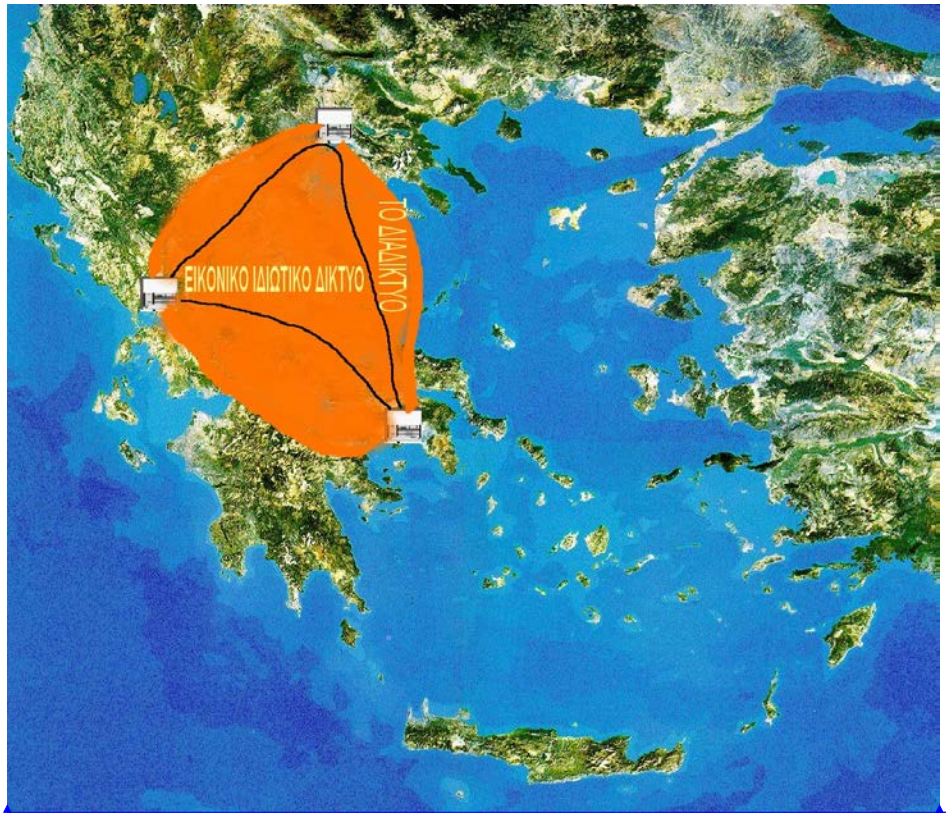
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

Εικόνα 1 Ένα τυπικό ιδιωτικό δίκτυο

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 στην εικόνα 1 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. Η εικόνα 2 αναπαριστάνει το ίδιο “συνεταιρικό” δίκτυο, αλλά αυτήν τη φορά χρησιμοποιούνται οι μηχανισμοί ασφαλείας ενός VPN, με το Internet ως WAN component.

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm



Εικόνα 2. Εικονικό Ιδιωτικό Δίκτυο

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial

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 της εικόνας 1, 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.

Formatted: Line spacing: 1,5 lines

Στο VPN όμως της εικόνας 2, αυτό που θα χρειάζονταν για την προσθήκη του επιπλέον site, θα ήταν ένας επιπλέον δρομολογητής, και κατάλληλη διαμόρφωση των ήδη υπάρχοντων δρομολογητών –απλή εργασία για ένα διαχειριστή δικτύου. Παρότι υπάρχει ένας μεγάλος αριθμός τεχνολογιών και πρωτοκόλλων που μπορούν να χρησιμοποιηθούν στην υλοποίηση ενός VPN, η πιο κοινή μορφή ενός VPN είναι αυτή που εμπεριέχει ένα encrypting firewall ή έναν encrypting router (δρομολογητής). Το firewall ή

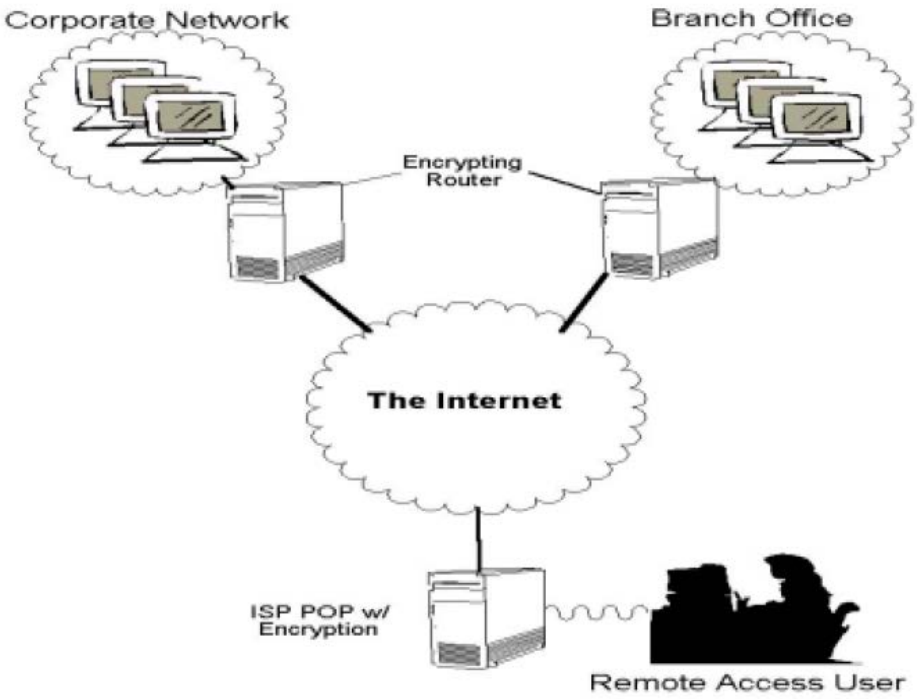
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Right: 0,63 cm

ο router δημιουργούν ένα κρυπτογραφημένο “tunnel” ή ασφαλές κανάλι στο Internet. Αυτό το tunnel, μαζί με ένα συμβατικό firewall και άλλους μηχανισμούς ασφαλείας, δημιουργούν μια “εικονική περίμετρο ασφαλείας” (virtual security perimeter) γύρω από το VPN. Το σχήμα 1 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 1 Μια λειτουργική όψη ενός VPN

Το μεγαλύτερο μειονέκτημα των VPN hardware και software είναι ότι δεν

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

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.

ΚΕΦΑΛΑΙΟ 6

ΑΣΦΑΛΕΙΑ ΛΟΓΙΣΜΙΚΟΥ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ

~~6.1 Ασφάλεια στο World Wide Web~~6.1 Ασφάλεια λειτουργικού συστήματος

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

- Αυθεντικοποίηση (Authentication)
- Έλεγχος προσπέλασης (Access Control)
- Έλεγχος ροής (Flow control)
- Έλεγχος Ορθότητας (Auditing)

Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial, Not Highlight
Formatted: Font: (Default) Arial, Not Highlight
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

- Προστασία μνήμης (Memory protection)

6.1.1 Αναγνώριση ταυτότητας/Αυθεντικοποίηση

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

- Συστήματα χρήσης συνθηματικού (password)
- Συστήματα "έρώτημα-απάντηση" (query-answer)
- Συστήματα διπλής αυθεντικοποίησης (two-way authentication)

Στα **συστήματα χρήσης password**, η αναγνώριση της ταυτότητας του χρήστη

πραγματοποιείται μέσω μιας μυστικής συμβολοσειράς γνωστής μόνο στο χρήστη και το σύστημα. Στα συστήματα πολλών χρηστών, τα passwords καταχωρούνται σε κάποιο αρχείο το οποίο διαχειρίζεται το Λ.Σ. Συνήθως προτιμάται η αποθήκευση των passwords σε μια περιοχή της μνήμης προσπελάσιμης μόνο από το Λ.Σ, όμως κάτι τέτοιο σημαίνει ότι όλα τα modules του Λ.Σ μπορούν να έχουν προσπέλαση στο αρχείο των passwords.

Έτσι, μη εξουσιοδοτημένοι χρήστες εκμεταλλευόμενοι ειδικά modules του Λ.Σ.

(trapdoors) θα μπορούσαν να προσπελάσουν το αρχείο. Ένα πρόσθετο μέτρο είναι η ύπαρξη ειδικών διαδικασιών login για προσπέλαση στο αρχείο των passwords. Όμως, και σε αυτήν την περίπτωση, μη εξουσιοδοτημένοι χρήστες θα μπορούσαν να διαβάσουν όλη τη μνήμη και συνεπώς την περιοχή εκείνη που περιέχει το συγκεκριμένο αρχείο.

Μειονεκτήματα της μορφής αυτής έχουν αντιμετωπιστεί με την κωδικοποίηση

των passwords με τη χρήση κρυπτογραφικών αλγορίθμων. Δηλαδή, τα passwords κωδικοποιούνται και καταχωρούνται στο αρχείο το οποίο μπορεί να ~~διαβασθεί~~διαβαστεί από όλους τους χρήστες, αλλά μόνο το Λ.Σ μπορεί να το τροποποιήσει (εισαγωγή, διαγραφή, ενημέρωση). Η προστασία του αρχείου επιτυγχάνεται με πολύπλοκους αλγόριθμους κρυπτογράφησης η αποκρυπτογράφηση των οποίων είναι σχεδόν αδύνατη.

Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

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

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

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

- Συστήματα δακτυλικών αποτυπωμάτων (fingerprint systems)
- Συστήματα φωτογραφιών χεριού (facsimile systems)
- Συστήματα αναγνώρισης φωνής (voice recognition systems)
- Συστήματα με τη βάθεια υπογραφής (hand-pressure systems)
- Συστήματα χαρακτηριστικών του αμφιβληστροειδούς (retinal features)

6.1.2 Έλεγχος προσπέλασης

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

Η προστασία της μνήμης και ο καταμερισμός ενός προγράμματος υλοποιείται

Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

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

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

Πίνακας προστασίας

Τα δικαιώματα προσπέλασης που παραχωρούνται στους χρήστες ή στις διεργασίες που ενεργοποιούνται από αυτούς (γνωστά ως υποκείμενα - subjects) πάνω σε αντικείμενα (objects) μπορούν να εκφραστούν μέσω ενός πίνακα προσπέλασης A (access matrix), ο οποίος αναπαρίσταται στο σχήμα 1. Οι γραμμές του πίνακα S1,…,SM αντιπροσωπεύουν τα υποκείμενα του συστήματος, ενώ οι στήλες O1, O2, …ON αντιπροσωπεύουν τα αντικείμενα του συστήματος (αρχεία, συσκευές I/O, προγράμματα).

	O1	O2	O3	O4	O5	…	…	ON
S1	r			r	r, w			
S2		r	w, r					
S3					r			x
…							r	
…	x							
SM			x					r, w

r = read, w = write, x = execute

Σχήμα 1 Ενδεικτικός πίνακας προστασίας

6.1.3 Έλεγχος ροής

Οι μηχανισμοί ελέγχου ροής (flow control) είναι υπεύθυνοι για τον έλεγχο των

δικαιωμάτων των χρηστών για προσπέλαση στους υπολογιστικούς πόρους, έτσι ώστε μόνο οι λειτουργίες που έχουν εγκριθεί να

Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

πραγματοποιούνται. Μέσω των μηχανισμών αυτών πραγματοποιείται η επαλήθευση του τελικού προορισμού των εξερχομένων μιας λειτουργίας ώστε να αποφεύγεται η διάδοση των πληροφοριών. Μια ροή πραγματοποιείται όταν οι πληροφορίες μετακινούνται από ένα αντικείμενο-πηγή σε ένα αντικείμενο-προορισμό.

Formatted: Font: (Default) Arial, Greek

Formatted: Line spacing: 1,5 lines

Γενικά, υπάρχουν δύο είδη ροής:

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

άμεση ή εσωτερική (explicit) και υπό συνθήκη ή εξωτερική (implicit). Η πρώτη πραγματοποιείται ως αποτέλεσμα εντολών μεταβίβασης,

y = f(x1, x2, …, xn)

ενώ η δεύτερη προκύπτει από εντολές συνθήκης,

if f(xm+1, …, xn) then y = f(x1, …, xm)

Οι μηχανισμοί ελέγχου ροής υλοποιούν τον έλεγχο με τον ορισμό μιας ετικέτας διαβάθμισης σε κάθε αντικείμενο, η οποία προσδιορίζει την κλάση ασφαλείας του αντικειμένου. Στη συνέχεια, οι ετικέτες χρησιμοποιούνται για την επαλήθευση των σχέσεων ροής που ορίζονται στο αντίστοιχο μοντέλο. Τέτοια μοντέλα είναι το μοντέλο προσπέλασης Bell-Lapadula και το μοντέλο Biba.

Formatted: Font: (Default) Arial, Greek

6.1.4 Προστασία μνήμης

Formatted: Font: (Default) Arial, 14 pt, Underline

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

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

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Συνήθως, η διαμοίραση περιλαμβάνει τα πρωτότυπα των δεδομένων και των

Formatted: Right: 0,63 cm

προγραμμάτων για εξοικονόμηση χώρου και χρόνου ενώ με ένα μοναδικό αντίγραφο η κατάσταση του αντικειμένου είναι πάντοτε ενημερωμένη και συνεπής.

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

- Ταυτόχρονη προσπέλαση (concurent access), δηλαδή ερωτήματα προσπέλασης για το
- ίδιο αντικείμενο, από διαφορετικούς χρήστες σε διαφορετικό χρόνο.
- Περιορισμένη προσπέλαση (confinement). Ισχύει μόνο για προγράμματα και αφορά την απαγόρευση αντιγραφής των παραμέτρων τους.
- Έτσι, ένα πρόγραμμα διαμοίρασης (π.χ ένας κειμενογράφος) παρεμποδίζεται στο να αντιγράφει και να μεταφέρει δεδομένα εισόδου σε αρχεία του συστήματος. Για παράδειγμα, μια τέτοια δυνατότητα θα ήταν εφικτή από την ύπαρξη ενός Trojan Horse στον κειμενογράφο.

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

- Μέθοδος φράγματος (fence address)
- Μέθοδος αναδιευθυνσης (relocation)
- Μέθοδος καταχωρητή (base/bound)
- Μέθοδος σελιδοποίησης (paging)
- Μέθοδος τμηματοποίησης (segmentation)

6.~~2~~1.5 Intrusion Detection Systems (ISD)

Ένα *Σύστημα Ανίχνευσης Εισβολής* ή IDS εν συντομία, επιχειρεί να ανιχνεύσει

έναν “κακόβουλο” χρήστη που εισβάλλει στο σύστημα, ή έναν νόμιμο χρήστη που προσπαθεί να εκμεταλλευθεί με κακό σκοπό τους πόρους του συστήματος ~~[72]~~. Ένα IDS εκτελείται μόνιμα στο σύστημα, συγκεκριμένα στο background, προειδοποιώντας τον administrator του συστήματος σε περίπτωση που ανιχνεύσει μια ύποπτη λειτουργία.

Υπάρχουν δύο κατηγορίες δυνητικών εισβολέων:

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

- **Έξωθεν εισβολείς (outside):** Οι περισσότεροι υπεύθυνοι συστημάτων σήμερα, θεωρούν την κατηγορία αυτή των εισβολέων ως τη μεγαλύτερη απειλή για την ασφάλεια των συστημάτων τους.
- **Εσωθεν εισβολείς (inside):** Μελέτες για λογαριασμό του FBI απέδειξαν ότι το 80% των εισβολών και των επιθέσεων προέρχονται από το εσωτερικό των επιχειρήσεων. Αυτό άλλωστε είναι κάτι φυσιολογικό, αφού οι έσωθεν γνωρίζουν καλύτερα από τον καθένα τη δομή των συστημάτων, ~~ποιά~~ποια και πόσα είναι τα πολύτιμα δεδομένα όπως και τους τρόπους που επιλέγονται για την προστασία τους.

Ένα υπολογιστικό σύστημα μπορεί να θεωρηθεί ως ένα σύνολο πόρων (resources) που είναι διαθέσιμοι στους εξουσιοδοτημένους χρήστες.

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Υπάρχουν έξι στοιχεία* στην ασφάλεια ενός συστήματος, που πρέπει να αποτελούν και το βασικό στόχο:

1) Διαθεσιμότητα -το σύστημα, όπως και ορισμένα κρίσιμα δεδομένα πρέπει να είναι διαθέσιμα για χρήση, όποτε οι νόμιμοι χρήστες τα χρειάζονται.

2) Χρησιμότητα -το σύστημα, και τα δεδομένα στο σύστημα, πρέπει να είναι χρήσιμα σε κάτι.

3) Ακεραιότητα -το σύστημα και τα δεδομένα του πρέπει να είναι πλήρη και σε αναγνώσιμη μορφή.

4) Αυθεντικοποίηση - το σύστημα πρέπει να είναι ικανό να πιστοποιήσει την ταυτότητα χρηστών και οι χρήστες θα πρέπει να μπορούν να πιστοποιήσουν την ασφάλεια του συστήματος.

5) Εμπιστευτικότητα - τα εμπιστευτικά δεδομένα πρέπει να είναι γνωστά μόνον στον ιδιοκτήτη των δεδομένων, ή σε οποιονδήποτε αυτός επιλέξει.

6) Κατοχή - οι ιδιοκτήτες του συστήματος πρέπει να μπορούν να το ελέγξουν.

Εαν ο έλεγχος του συστήματος περιέλθει σε έναν “κακόβουλο” χρήστη, αυτομάτως ~~επηρεάζονται~~επηρεάζονται όλοι οι χρήστες που σχετίζονται με το σύστημα.

Με βάση τα παραπάνω, **μια εισβολή,** μπορεί να θεωρηθεί ~~ώς~~ως **ένα σύνολο ενεργειών με σκοπό να παραβιαστεί η ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα ενός πόρου**.

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

- **Εκμετάλλευσης** (misuse), που είναι καλά ορισμένες επιθέσεις σε αδύναμα σημεία ενός συστήματος. Μπορούν να ανιχνευθούν με την εξέταση ~~εαν~~εάν έχουν πραγματοποιηθεί συγκεκριμένες πράξεις σε

Formatted: Right: 0,63 cm

συγκεκριμένα αντικείμενα του συστήματος. Οι εισβολές αυτές ακολουθούν γνωστά μοντέλα (patterns), επομένως ο συστηματικός έλεγχος των log αρχείων μπορεί να οδηγήσει εύκολα στην ανίχνευσή τους.

- ~~Ανωμαλίας~~Ανωμαλίας (anomaly), που συνίστανται απλά σε παρεκκλίσεις από τη συνήθη λειτουργία του συστήματος. Ανιχνεύονται με τη δημιουργία ενός profile του συστήματος το οποίο ελέγχεται, και κατόπιν ελέγχοντας το αν και κατά πόσον υπάρχουν παρεκκλίσεις από αυτό το profile. Οι εισβολές αυτές είναι δύσκολο να ανιχνευτούν.

Δεν υπάρχουν σταθερά μοντέλα που να μπορούν να χρησιμοποιηθούν με βεβαιότητα ως σημεία αναφοράς. Έτσι, τα IDS πρέπει να να ~~υϊοθετούν~~υιοθετούν μια "ασαφή" λογική (fuzzy logic) στην προσέγγιση των εισβολών αυτού του είδους. Πολλά IDS βασίζουν τη λειτουργία τους στην ανάλυση των ελέγχων ορθότητας του λειτουργικού συστήματος. Ένα IDS μπορεί επίσης να ασκεί τον δικό του έλεγχο του συστήματος, ~~συσγκεντρώνοντας~~συγκεντρώνοντας καταρχήν ένα σύνολο στατιστικών που καταγράφουν το profile της χρήσης του συστήματος. Τα στατιστικά αυτά στοιχεία μπορούν να εξαχθούν από μια ποικιλία πηγών, όπως η χρήση της CPU, των συσκευών I/O, της μνήμης, οι δραστηριότητες των χρηστών, ο αριθμός των logins, κ.λ.π. Αυτά τα στατιστικά πρέπει να ενημερώνονται συνεχώς ώστε να αντανακλούν τη τρέχουσα κατάσταση του συστήματος.

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

1. Πρέπει να **εκτελείται συνεχώς** χωρίς ανθρώπινη επιτήρηση. Το σύστημα πρέπει να είναι αρκετά αξιόπιστο ώστε να του επιτρέπεται η εκτέλεση στο background. Εντούτοις, δεν πρέπει να είναι ένα "black box": οι εσωτερικές του λειτουργίες πρέπει να επιδέχονται εξέτασης από τους "έξω".

2. Πρέπει να είναι **ανθεκτικό** υπό την έννοια ότι θα πρέπει να ~~αντεπεξέλθει~~ανταπεξέλθει έπειτα από μια π.χ κατάρρευση του συστήματος, χωρίς να χρειάζεται να ξανα-χτίσει την βάση γνώσης του.

3. Πρέπει να **αυτοελέγχεται**, δηλαδή να ελέγχει τις λειτουργίες του, για την περίπτωση που έχει παραβιαστεί από κάποιον.

Formatted: Font: (Default) Arial, Bold
Formatted: Font: (Default) Arial
Formatted: Font: Bold
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

4. Πρέπει να επιβαρύνει το σύστημα με το **ελάχιστο φόρτο**. Ένα IDS που καταναλώνει μεγάλες ποσότητες υπολογιστικών πόρων, ζημιώνει περισσότερο από ό,τι προσφέρει.

5. Πρέπει να είναι **προσαρμόσιμο** στις ανάγκες του συστήματος στο οποίο χρησιμοποιείται. Κάθε σύστημα έχει ένα διαφορετικό μοντέλο χρήσης, οπότε και οι μηχανισμοί άμυνας πρέπει να προσαρμόζονται σε αυτά τα ~~μοντάλα~~μοντέλα.

6. Δεν πρέπει να "ξεγελιέται" εύκολα.

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

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

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

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

~~**6.3 Ασφάλεια Server**~~

~~*Πρόσφατη έρευνα (Μάρτιος 1997) που έκανε ο κ. Dan Farmer σε 2200 από τα πιο*~~

~~*γνωστά World Wide Web sites βρήκε αδυναμίες στα συστήματα ασφαλείας των δύο τρίτων από αυτά (66%). Ένα επιπλέον ποσοστό της τάξης του 9-24%*~~

Formatted: Right: 0,63 cm

~~*θεωρείται σχετικά επισφαλές με την έννοια ότι θα αντιμετωπίσει προβλήματα αν βρεθεί το παραμικρό bug σε ένα ή δύο από τα πιο δημοφιλή προγράμματα της αγοράς (κάτι που ως γνωστόν συμβαίνει αρκετά συχνά). Παρ' όλο που δεν έγινε καμμία προσπάθεια να αποκρυφθεί το γεγονός ότι γινόταν η έρευνα, μόνο 3 από τα 2200 sites στα οποία έγινε η έρευνα αντέδρασαν προσπαθώντας να βρουν ποιός την πραγματοποιούσε και γιατί .*~~

~~6~~6.1.6 ~~.3.1~~ Ασφάλεια Web Server

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

Δικαιώματα (file permissions)

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

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

Το **server root** πρέπει να διαμορφωθεί ώστε μόνον ο χρήστης www να μπορεί να γράψει στους καταλόγους των αρχείων διαμόρφωσης και καταγραφής, αλλά και στα περιεχόμενά τους. Έγκειται στον διαχειριστή να αποφασίσει ~~εαν~~εάν οι κατάλογοι αυτοί πρέπει να είναι αναγνώσιμοι από την ομάδα www. Το σίγουρο είναι ότι δεν πρέπει να

Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

είναι αναγνώσιμοι από όλους (world-readable). Ο κατάλογος cgi-bin και τα περιεχόμενά του πρέπει να είναι εκτελέσιμα και αναγνώσιμα από όλους, αλλά όχι εγγράψιμα (writable). Στη συνέχεια ακολουθεί ένα παράδειγμα για τα δικαιώματα στο server root:

```
drwxr-xr-x   5 www      www         1024  Aug  8  00:01 cgi-bin/
drwxr-x---   2 www      www         1024  Jun  11 17:21  conf/
-rwx------   1 www      www       109674  May  8  23:58  httpd

drwxrwxr-x   2 www      www         1024  Aug  8   00:01  htdocs/
drwxrwxr-x   2 www      www         1024  Jun   3  21:15  icons/
drwxr-x---   2 www      www         1024  May  4   22:23  logs/
```

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Το **document root** χρειάζεται διαφορετική αντιμετώπιση. Όλα τα αρχεία που

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Greek

Formatted: Font: (Default) Arial

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

Formatted: Line spacing: 1,5 lines

```
drwxrwxr-x   3 www      www         1024    Jul   1   03:54  contents
drwxrwxr-x  10 www      www         1024    Aug  23 19.32  examples
-rw-rw-r--   1 www      www         1488    Jun  13  23:30  index.html
-rw-rw-r--   1 lstein    www        39224    Jun  11  23:00  resource_guide.html
```

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Εκτέλεση του server (running the server)

Καθημερινά εγείρονται πολλές διαφωνίες στο Internet σχετικά με την ταυτότητα

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

χρήστη υπό την οποία πρέπει να εκτελείται ο Web server. Οι περισσότεροι servers

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

εκτελούνται ως root ώστε να μπορούν να “ανοίξουν” την port 80 (η standard HTTP port) και να γράψουν στα log αρχεία. Στη συνέχεια, αναμένουν για μια εισερχόμενη σύνδεση στην port 80. Μόλις λάβουν τη σύνδεση, “εξ-ωθούν” (fork) μια υπο-διαδικασία (child process) να αναλάβει την αίτηση, και επιστρέφουν σε κατάσταση αναμονής. Η υπο-διαδικασία αυτή εντωμεταξύ,

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

μεταβάλλει το ID χρήστη της σε αυτό του χρήστη “nobody” και κατόπιν χειρίζεται την αίτηση. Όλες οι ενέργειες που γίνονται ως απάντηση στις αιτήσεις του απομακρυσμένου χρήστη, όπως η εκτέλεση CGI scripts ή Server-Side Includes, γίνονται με τα δικαιώματα του χρήστη “nobody” (μη προνομιούχος χρήστης).

Ο κίνδυνος υφίσταται, όχι τόσο όταν ο server εκτελείται ως root, αλλά όταν ο

server έχει διαμορφωθεί ώστε η υπο-διαδικασία (child process) να εκτελείται με

δικαιώματα root (καθορίζοντας “User root” στο αρχείο διαμόρφωσης του server). ~~Εαν~~Εάν

συμβαίνει κάτι τέτοιο, τότε π.χ κάθε CGI script θα έχει δικαιώματα root, με

καταστροφικά αποτελέσματα.

Ορισμένοι υποστηρίζουν πως δεν πρέπει ούτως ή άλλως να εκτελείται ο server ως

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

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

Web και ftp Servers

Πολλά sites αρέσκονται στο να διατηρούν το ίδιο “δένδρο εγγράφων” (document

tree) τόσο για τον Web όσο και για τον FTP server. Αυτό δεν συνιστά απαραίτητα

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

"τρύπα" ασφαλείας, **αρκεί να μην υπάρχει τρόπος** ένας χρήστης να κάνει upload αρχεία τα οποία αργότερα θα μπορέσει να αναγνώσει ή εκτελέσει με τον Web daemon.

Ας θεωρήσουμε το εξής σενάριο: ο WWW server έχει διαμορφωθεί ώστε να

εκτελεί οποιοδήποτε αρχείο με την κατάληξη '.cgi'. Χρησιμοποιώντας τον ftp daemon, ένας απομακρυσμένος hacker κάνει upload ("ανεβάζει") ένα perl script στο ftp site, δίνοντας του την κατάληξη '.cgi'. Στη συνέχεια χρησιμοποιεί τον browser του και ζητά από τον Web server την εκτέλεση του αρχείου που μόλις ανέβασε. Έτσι, έχει παρακάμψει την ασφάλεια του συστήματος και εκτελεί εντολές τις αρεσκείας του. Τα ftp uploads πρέπει να περιορίζονται σε ένα συγκεκριμένο κατάλογο, ο οποίος

να μη μπορεί να διαβαστεί από το χρήστη "nobody".

Ασφάλεια και Web Search Engines

Σήμερα οι μηχανές αναζήτησης (π.χ Yahoo, Google, Lycos) έχουν γίνει περισσότερο

ισχυρές από ποτέ* . Ορισμένα Web sites παρέχουν πολλά links, συμπεριλαμβανομένων και πληροφοριών που αφορούν τις ρυθμίσεις του συστήματος. Για παράδειγμα, εάν κάποιος κάνει μια έρευνα με μια από αυτές τις μηχανές αναζήτησης, με λέξεις κλειδί 'root', 'daemon', 'passwd', κ.λ.π, τότε η μηχανή αναζήτησης ενδεχομένως να εμφανίσει μια λίστα από αρχεία /etc/passwd ή /etc/group, τα οποία βρίσκονται σε συστήματα με "αδύναμες" ρυθμίσεις και μηχανισμούς ασφαλείας. Έτσι, αυτός είναι ένας γρήγορος τρόπος να ανακαλυφθούν τα ευάλωτα συστήματα στο Internet. Οι Web administrators πρέπει να είναι προσεκτικοί σχετικά με το τί είδους πληροφορία είναι διαθέσιμη στο Internet, ενώ δεν πρέπει να υπάρχουν URLs που οδηγούν σε εμπιστευτικές πληροφορίες.

6.~~3.2~~1.7 Ασφάλεια anonymous FTP Server

Το File Transfer Protocol, ή FTP, αποτελεί τη βάση για τον αρχαιότερο τύπο

υπηρεσίας στο Internet, τον anonymous FTP server ~~[73]~~. Οι anonymous FTP servers

επιτρέπουν μη εξουσιοδοτημένη πρόσβαση σε ένα τμήμα του συστήματος αρχείων (file system) του host. Το software του server επιτρέπει

Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial, 14 pt, Underline, Greek
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

σε απομακρυσμένους χρήστες να ανακτούν αρχεία, περιστασιακά να "ανεβάζουν" (upload) αρχεία, ή ακόμα και πιο προηγμένες λειτουργίες όπως συμπίεση αρχείων.

Αδυναμίες του anonymous FTP Server

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

- Χρήστες στο Internet ενδέχεται να χρησιμοποιούν εγγραφές περιοχές στο FTP σύστημα αρχείων ώστε να ανταλλάσουν αρχεία. Αυτή είναι μια συνήθης τεχνική για ανταλλαγή παράνομου ή copyrighted software, καθώς και πορνογραφικών εικόνων.
- Οι χρήστες μπορούν να αλλάξουν/σβήσουν πληροφορίες software.
- Στο παρελθόν, ανακαλύφθησαν αδυναμίες στο FTP software, οι οποίες επέτρεπαν πλήρη πρόσβαση στα αρχεία του συστήματος** . Αυτές οι αδυναμίες εξαλείφθησαν αλλά καθώς προστίθενται συνεχώς καινούρια χαρακτηριστικά στο software, είναι πιθανή η εμφάνιση άλλων αδυναμιών.

- Λάθη στις ρυθμίσεις (configuration errorrs) ενδέχεται να επιτρέπουν πρόσβαση σε εμπιστευτικά αρχεία. Για παράδειγμα, ένα σύνηθες λάθος στη διαμόρφωση του anonymous FTP server είναι όταν ένα αντίγραφο του αρχείου passwords του συστήματος τοποθετείται σε περιοχή διαθέσιμη στους απομακρυσμένους χρήστες. Εαν οι τοπικοί χρήστες έχουν επιλέξει "αδύναμα" passwords, οι εισβολείς μπορούν να χρησιμοποιήσουν το αρχείο passwords ώστε να παραβιάσουν το σύστημα.

Ρυθμίσεις του anonymous FTP Server

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

- Δεν πρέπει να υπάρχουν αρχεία κατάλογοι στην anonymous FTP περιοχή (area), που να ανήκουν στον χρήστη 'ftp'. Αυτό είναι το ID των anonymous χρηστών, κα ιο,τιδήποτε ανήκει σε αυτό το ID μπορεί να τροποποιηθεί να αντικατασταθεί, ή να σβηστεί από κάποιον απομακρυσμένο χρήστη στο Internet.

Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

- Δεν πρέπει να υπάρχουν κρυπτογραφημένα passwords από το αρχείο passwords του συστήματος (/etc/passwd) στο αρχείο passwords της anonymous FTP περιοχής (~ftp/etc/passwd). Οποιοσδήποτε από το Internet θα μπορούσε να αποκτήσει τα κρυπτογραφημένα αυτά passwords, και να προσπαθήσει να τα αποκρυπτογραφήσει.
- □Εαν ε□αιδυνατ□, δε θα π ρ□πειν α επ τρ□πεται εγγραφ□σε αρχε□α□ καταλόγους από anonymous χρήστες.

6.41.8 Ασφάλεια Browser

Για τους περισσότερους, το Internet είναι ο νοητός εκείνος χώρος όπου εκτελούν

κυρίως αυτό που ονομάστηκε “surfing” . Ένα από τα σημαντικά πεδία ανταγωνισμού

των επίδοξων κηδεμόνων του χώρου, αποτέλεσε και αποτελεί το λογισμικό που

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

~~Στο κεφάλαιο 4 αναφερθήκαμε διεξοδικά για ορισμένες παραβιάσεις ασφαλείας~~

~~που σχετίζονταν με αδυναμίες των δημοφιλών Web browsers στην ενσωμάτωση της Java τεχνολογίας. Τα λάθη αυτά είναι χαρακτηριστικά των αδυναμιών που παρουσιάζουν οι browsers που διατίθενται στο Web.~~ ~~Εδώ~~Παρακάτω, θα παρουσιάσουμε ενδεικτικά δύο ~~ακόμη~~ παραβιάσεις, που ~~δεν αφορούν τη Java, αλλά~~ είναι ~~εξίσου~~αρκετά χαρακτηριστικές:

Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial, 14 pt, Underline, Greek
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

- Τον Απρίλιο 1997, ανακαλύφθηκε ένα σοβαρό πρόβλημα του **Internet Explorer 3.01*** το οποίο επιτρέπει στους συγγραφείς σελίδων web να χρησιμοποιήσουν αρχεία τύπου .URL και .LNK για να τρέξουν προγράμματα στον υπολογιστή του αναγνώστη (client), με όλες τις συνεπακόλουθες δυνατές συνέπειες. Μάλιστα, η περίπτωση των αρχείων .URL είναι πιο επικίνδυνη, διότι τα αρχεία αυτά τρέχουν και σε Windows NT. Επίσης, τα client side scripts μπορούν να χρησιμοποιήσουν το αντικείμενο 'Explorer' για να μεταφέρουν ένα αρχείο batch στον υπολογιστή του χρήστη και στη συνέχεια να το εκτελέσουν.
- Τον Ιούλιο του 1997, ανακαλύφθηκε ένα πρόβλημα του **Netscape Navigator 4.0**** , το οποίο επιτρέπε σε ένα hacker να παρατηρεί τη δραστηριότητα ενός χρήστη στο Web: να παρακολουθεί τα URLs που "επισκέφτεται" ο χρήστης, τα δεδομένα που εισάγει στις HTML φόρμες (συμπεριλαμβανομένων) και των passwords, όπως και τα δεδομένα που τοποθετούνται στο cookie αρχείο του χρήστη ~~(παράγραφος .5)~~.

Τρεις από τους πιο δημοφιλείς Web browsers, είναι ο Netscape Navigator, ο

Microsoft Internet Explorer, και ο HotJava .

Ο **Netscape Navigator** χρησιμοποιεί την SSL (Secure Sockets Layer) τεχνολογία,

παρέχοντας προστασία των δεδομένων που ανταλλάσονται μεταξύ browser και server, με τη χρήση κρυπτογραφίας δημόσιου κλειδιού, και πιστοποιητικών (certificates). Επίσης, υποστηρίζει τον SOCKS server, καθιστώντας ένα firewall διάφανο στον χρήστη. Στον Navigator, τα ασφαλή URLs αρχίζουν με το πρόθεμα 'https://', αντί για το κλασσικό 'http://', ενώ όταν ο χρήστης μεταβαίνει σε ένα site που υποστηρίζει SSL, ενεργοποιείται ένα εικονίδιο στο κάτω αριστερά σημείο του browser interface. Στον Netscape Navigator, υπάρχουν μενού επιλογών για ρυθμίσεις που αφορούν θέματα ασφαλείας, όπως για παράδειγμα προειδοποίηση πριν την εκτέλεση applets ή ActiveX προγραμμάτων. Όταν ο Navigator δεν μπορεί να κάνει μια ασφαλή σύνδεση, εμφανίζει στην οθόνη του χρήστη ένα προειδοποιητικό pop-up παράθυρο, επιτρέποντας στον χρήστη να ακυρώσει την συνέχεια της μετάδοσης. Τέλος, υποστηρίζει την τεχνολογία S/MIME για ανταλλαγή email.

Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, French (France)
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, French (France)
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

.

Ο **Internet Explorer**, που περιλαμβάνεται ~~στα~~ στα Windows ~~95~~, υποστηρίζει ~~τις~~ τις

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

Ο **HotJava browser** ενσωματώνει πλήρως την τεχνολογία της Java. Έχει τη

δυνατότητα να προσαρμόζεται γρήγορα σε καινούρια πρωτόκολλα, χωρίς να περιορίζεται σε συγκεκριμένες λειτουργίες. Λειτουργεί ως ένας “έξυπνος” interpreter εκτελέσιμου περιεχομένου, ικανός να εμφανίζει καινούρια formats. Ο Hotjava κληρονομεί τα χαρακτηριστικά ασφαλείας της Java, όπως περιορισμό πρόσβασης στη μνήμη, πιστοποίηση bytecodes και Security Manager ~~(κεφάλαιο 4)~~. Έχει δυνατότητα χρήσης κρυπτογραφικών μηχανισμών δημόσιου κλειδιού, ενώ μπορεί να διακρίνει εαν το bytecode προέρχεται μέσα ή έξω από το firewall.

Αρμοδιότητες των χρηστών

Παρά το γεγονός ότι, αν υπάρχει ένα λάθος στον κώδικα του browser τότε οι

χρήστες είναι σχετικά “απροστάτευτοι”, υπάρχουν ορισμένα μέτρα πρόληψης :

1) Οι χρήστες πρέπει να κάνουν συχνά backup στα εμπιστευτικά τους αρχεία. Οι

σύγχρονοι δίσκοι δε χαλάνε εύκολα, αλλά είναι ευάλωτοι από άλλες πλευρές.

2) Οι χρήστες πρέπει να “μοιράζουν” στο δίκτυο μόνο ότι είναι εντελώς απαραίτητο, και για όσο λιγότερο χρόνο γίνεται. Τα σημαντικά αρχεία πρέπει να κρατούνται όσο

γίνεται μακριά από (ακόμα και φυσική, αν είναι δυνατόν) προσπέλαση τρίτων.

Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

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

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

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

~~6.5~~6.1.9 HTTP Cookies

Η πλήρης ονομασία των cookies είναι Persistent Client State HTTP Cookies ~~[77]~~.

Ουσιαστικά, ένα cookie είναι δεδομένα που στέλνει ο server στον browser, όταν ο δεύτερος επισκέπτεται ένα Web site για πρώτη φορά. Τα δεδομένα αυτά ο browser τα αποθηκεύει καταρχήν στη μνήμη, και κατόπιν στο σκληρό δίσκο. Ο browser στη συνέχεια επιστρέφει αυτά τα δεδομένα στον server, ως τμήμα **κάθε αίτησης** προς τον server.

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

Εντοπίζουμε δύο σημαντικά τμήματα σε ένα cookie: Το *Name* (όνομα) και το

Formatted ... (×64)

Value (τιμή). Όταν ένα CGI πρόγραμμα διαβάζει την μεταβλητή περιβάλλοντος

HTTP_COOKIE, εντοπίζει ένα απλό string που περιέχει όλα τα cookies που έστειλε ο

browser. Κάθε cookie αποτελείται από ένα ζεύγος *Name=Value*, και χωρίζεται από τα

άλλα με ένα ερωτηματικό (';'). Τα περιεχόμενα του HTTP_COOKIE για μια αίτηση με ένα απλό cookie, θα μοιάζουν ως εξής:

IDENTITY=19970117.WPI.1034

και για δυο cookies:

IDENTITY=19970117.WPI.1034 ; CLUB_PREFERENCES=0-2-3-17-1-23-A-5-14

Στο δεύτερο παράδειγμα φαίνεται πώς τα δυο cookies έχουν διαφορετικά ονόματα και

περιέχουν διαφορετικά δεδομένα. Επεξεργαζόμενος τις πληροφορίες ενός ή

περισσότερων cookies, ο server μπορεί να καθορίσει τί θα σταλεί πίσω στον χρήστη, και να αναλύσει τη δραστηριότητα του χρήστη, κάτι που θα ήταν δυσκολότερο ή αδύνατο χωρίς τη χρήση των cookies.

Αποθηκεύοντας πληροφορίες σε βάση δεδομένων

Συνήθως, οι πληροφορίες που αποκτώνται από τα cookies καταχωρούνται σε μια

βάση δεδομένων, για περαιτέρω επεξεργασία. Για το σκοπό αυτό, μπορούν να

χρησιμοποιηθούν εργαλεία αποθήκευσης δεδομένων όπως mSQL, Informix, Oracle,

Sybase. Το ερώτημα που τίθεται, είναι "ποιά πληροφορία θα χρησιμοποιηθεί ως κλειδί για την προσπέλαση της βάσης". Η απάντηση είναι απλή: αν υποθέσουμε ότι ο χρήστης συμπληρώνει δεδομένα σε μια HTML φόρμα, και ότι το CGI script που χειρίζεται το input του χρήστη βρίσκεται σε μια περιοχή του server που απαιτεί οι χρήστες να συνδέονται (log-in) μέσω βασικής αυθεντικοποίησης, τότε μπορεί να χρησιμοποιηθεί η μεταβλητή περιβάλλοντος REMOTE_USER.

Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

Συνδυάζοντας τα cookies με τη βάση δεδομένων

Στο προηγούμενο παράδειγμα, αποθηκεύσαμε πληροφορίες για τον χρήστη σε μια

βάση δεδομένων στον Web server, τις οποίες πληροφορίες μπορούμε να ανακτήσουμε όποτε επιθυμούμε. Ένα προφανές χρονικό σημείο που θα επιθυμούσαμε να ανακτήσουμε την πληροφορία αυτή, θα ήταν η στιγμή που ο χρήστης επιστρέφει στο site. Σε αυτήν τη στιγμή, θα θέλαμε να γνωρίζουμε ότι ο συγκεκριμένος χρήστης έχει επισκεφτεί το site στο παρελθόν. Εαν αυτό ισχύει, συγκεντρώνουμε πληροφορίες για το χρήστη και τις χρησιμοποιούμε για να αλλάξουμε την HTML σελίδα που του στέλνουμε.

Εαν ο χρήστης έχει δεχθεί ένα cookie που περιέχει το USER ID του, τότε μπορούμε να χρησιμοποιήσουμε την πληροφορία αυτή στο cookie ως κλειδί για την

προσπέλαση της εγγραφής του χρήστη στη βάση δεδομένων. Στο προηγούμενο

παράδειγμα, ο server απέκτησε το όνομα του χρήστη χάρη στη βασική αυθεντικοποίηση. Σε αυτό το παράδειγμα, χρησιμοποιώντας το cookie, ο server μπορεί να αποκτήσει το όνομα του χρήστη χωρίς ο χρήστης να πρέπει να ξανα-αυθεντικοποιηθεί.

6.51.10 Ασφάλεια και cookies

Σήμερα τα cookies δημιουργούν αρκετές τριβές στην κοινότητα των χρηστών του

Web . Υπάρχουν ορισμένοι που πιστεύουν ότι τίθεται θέμα εμπιστευτικότητας των

πληροφοριών και ιδιωτικής ζωής των χρηστών, που δέχονται σε μεγάλη ποσότητα και

συνήθως χωρίς καμία προειδοποίηση cookies από Web servers. Η αλήθεια είναι πως

παρότι τα cookies υποστηρίζονται από τον Netscape Navigator και τον Internet Explorer από τις αρχές του 1996, η ύπαρξή τους έμεινε μυστική για αρκετά μεγάλο χρονικό διάστημα από τους χρήστες, κάτι που προκάλεσε πολλά ερωτηματικά. Η μόνη ένδειξη ύπαρξής τους, είναι ένα αρχείο που καλείται ‘cookies.txt’, το οποίο θα εντοπίσουν στο σκληρό τους όλοι οι χρήστες των δυο δημοφιλών browsers.

Formatted: Line spacing: 1,5 lines

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Greek

Formatted: Font: (Default) Arial

Formatted: Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, 14 pt, Underline

Formatted: Font: (Default) Arial, 14 pt, Underline, Greek

Formatted: Font: (Default) Arial, 14 pt, Underline

Formatted: Font: (Default) Arial, 14 pt, Underline, Greek

Formatted: Font: (Default) Arial, 14 pt, Underline

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

Εντούτοις, από την έκδοση του Navigator 3.0 και έπειτα, οι χρήστες μπορούν να

διαμορφώσουν τον browser ώστε να τους προειδοποιεί ότι ένα απομακρυσμένο site

επιχειρεί να εισάγει πληροφορίες στο αρχείο cookie.txt* . Βέβαια, αυτή η πληροφόρηση δημιουργεί ~~σύγχιση~~ σύγχυση σε αρκετές περιπτώσεις. Έτσι, για παράδειγμα, ο χρήστης User μπορεί να προειδοποιηθεί ότι ο server1.com επιχειρεί να τροποποιήσει το cookie αρχείο, ενώ ο User, αφενός τη στιγμή που δέχεται την προειδοποίηση δεν είναι σε μια σελίδα του server1.com, αφετέρου δεν έχει επισκεφθεί ποτέ μια σελίδα του server1.com. Η πολύ απλή εξήγηση είναι οι διαφημ~~ή~~ίσεις που κατακλύζουν σήμερα τα Web sites. Ο server1.com, προφανώς διαφήμιζε ένα προϊόν του στη σελίδα που επισκέφτηκε ο User (κατόπιν εμπορικής συμφωνίας με τον server που φιλοξενεί τη διαφήμιση), και επιθυμούσε, την επόμενη φορά που ο User θα επισκεφτόταν την ίδια σελίδα μην έβλεπε την ίδια διαφήμιση αλλά μια άλλη διαφήμιση προϊόντος του.

Συχνά, ορισμένα sites αποθηκεύουν στο cookies.txt του χρήστη εμπιστευτικές

πληροφορίες όπως το password του χρήστη ή κωδικούς πιστωτικών καρτών. Με ~~τις~~τις

τεχνολογίες που υπάρχουν σήμερα στο Web, ο σκληρός δίσκος του χρήστη δεν είναι

πλέον ασφαλής, πόσο μάλλον το αρχείο cookies.txt, το οποίο βρίσκεται πάντα σε

συγκεκριμένο κατάλογο στο δίσκο. Επομένως, τα sites που αποθηκεύουν σημαντικές

πληροφορίες, θα έπρεπε να προειδοποιούν το χρήστη, ώστε να προστατεύσει το αρχείο από μη εξουσιοδοτημένη πρόσβαση.

Πολλοί υποστηρίζουν πως δεν έχει αποσαφηνιστεί αρκετά ο τρόπος λειτουργίας

των cookies, και οι δυνατότητες που έχουν . Σίγουρα, το γεγονός ότι οι Web servers

απέκτησαν το δικαίωμα να “γράφουν” στο σκληρό δίσκο των ανυποψίαστων χρηστών, προβληματίζει αρκετούς. Αν μάλιστα λάβουμε υπ’όψιν μας και το γεγονός ότι χιλιάδες διαφημιστικά e-mails στέλνονται

Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

καθημερινά σε χρήστες, με βάση πληροφορίες που αναγράφονται στα cookies, τότε ο προβληματισμός αυτός γίνεται μεγαλύτερος .

Διατήρηση Ανωνυμίας

Στο Web διατίθενται ορισμένα προγράμματα εμπορικά ή δωρεάν, που βοηθούν

τους χρήστες να διατηρήσουν την ανωνυμία τους, κατά την περιήγησή τους στο Web.

Δύο από αυτά τα προϊόντα είναι το NSClean και IEClean (http://www.axxis.com/), τα

οποία μπορούν να σβήσουν από το σκληρό δίσκο του χρήστη cookies, bookmarks,

history και τη cashe. Ένα άλλο προϊόν το PGPcookie.cutter (http://www.pgp.com/) έχει παρόμοια λειτουργία, συν του ότι διατίθεται ως plug-in του browser.

Ένα προϊόν που διατίθεται δωρεάν είναι ο Anonymizer (www.anonymizer.com/),

που στη λειτουργία του προσομοιώνει έναν anonymous proxy server, εμποδίζοντας τον εντοπισμό της ταυτότητας των χρηστών.

6.2 Ασφάλεια στο UNIX

6.2.1 Ιστορία της Ασφάλειας του Unix

Όταν μιλάμε για την ασφάλεια του Unix θα πρέπει να έχουμε λάβει υπόψη μας ότι το Unix δεν είχε σχεδιαστεί από την αρχή να είναι ασφαλές. Σχεδιάστηκε έτσι ώστε να έχει τα απαραίτητα χαρακτηριστικά που να το κάνουν λειτουργικό.

Το Unix είναι ένα πολυ-χρηστικό *(multi-user)* και πολυ-διεργασιακό *(multi-tasking)* λειτουργικό σύστημα. Πολυ-χρηστικό σημαίνει ότι το λειτουργικό σύστημα επιτρέπει σε πολλούς διαφορετικούς χρήστες να χρησιμοποιούν το ίδιο υπολογιστικό σύστημα την ίδια στιγμή. Πολυ-διεργασιακό σημαίνει ότι ο κάθε ένας από αυτούς τους χρήστες μπορεί να τρέχει ταυτόχρονα πολλά διαφορετικά προγράμματα.

Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 14 pt, Not Italic, Underline, Greek
Formatted: Font: (Default) Arial, 14 pt, Not Italic, Underline
Formatted: Font: (Default) Arial, 14 pt, Not Italic, Underline, Greek
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial, Underline, Greek
Formatted: Font: (Default) Arial, Greek
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Right: 0,63 cm

Μία από τις πιο κοινές διεργασίες τέτοιων λειτουργικών συστημάτων είναι η αποτροπή των παρεμβολών μεταξύ των διαφόρων χρηστών. Χωρίς μία τέτοιου είδους προστασία κάποιος χρήστης θα μπορούσε να επηρεάσει τον τρόπο λειτουργίας προγραμμάτων άλλων χρηστών με αποτέλεσμα το σβήσιμο αρχείων ή χειρότερα το "ρίξιμο" *(crush-halt)* της μηχανής. Για την αποφυγή τέτοιων καταστροφών το Unix είχε πάντα ενσωματωμένη κάποια μορφή ασφάλειας στη φιλοσοφία σχεδίασής του.

Ωστόσο το Unix παρέχει πολλά παραπάνω από μία μερική προστασία. Το Unix έχει ένα ανεπτυγμένο σύστημα ασφάλειας με το οποίο ελέγχει τον τρόπο με τον οποίο οι χρήστες αποκτούν πρόσβαση στους λογαριασμούς και στα αρχεία τους, κάνουν αλλαγές σε βάσεις δεδομένων και χρησιμοποιούν τους πόρους του συστήματος. Ατυχώς, αυτοί οι μηχανισμοί δεν βοηθούν και πολύ όταν τα συστήματα έχουν ρυθμιστεί λανθασμένα ή χρησιμοποιούνται απρόσεκτα και περιέχουν μη ελεγμένο λογισμικό.

6.2.2 Χρήστες και Passwords

Κάθε άτομο που χρησιμοποιεί ένα Unix σύστημα πρέπει απαραίτητα να έχει λογαριασμό *(account)* σε αυτό το σύστημα. Οι λογαριασμοί αναγνωρίζονται από ένα μοναδικό όνομα-χρήστη *(username)*. Παραδοσιακά κάθε λογαριασμός έχει επιπλέον ένα μυστικό κωδικό *(password)* που σχετίζεται άμεσα με αυτόν και αποτρέπει την παράνομη χρήση του. Ένας χρήστης πρέπει να γνωρίζει απαραίτητα τόσο το *username* όσο και το *password* του για να αποκτήσει πρόσβαση στο Unix σύστημα.

Το username είναι ένα στοιχείο με το οποίο το σύστημα παίρνει την ταυτότητά μας ενώ το password είναι το αποδεικτικό στοιχείο αυτής. Τα κανονικά usernames έχουν από έναν έως και οκτώ χαρακτήρες. Σε έναν υπολογιστή που έχει για λειτουργικό το Unix τα usernames διαφορετικών χρηστών πρέπει να είναι διαφορετικά ενώ τα passwords, τα οποία επίσης αποτελούνται από έναν έως οκτώ χαρακτήρες, αν και πρέπει να είναι διαφορετικά μπορεί και να είναι ίδια κάτι που σημαίνει ωστόσο ότι και οι δύο χρήστες που έχουν τον ίδιο κωδικό έχουν κάνει λάθος και μάλιστα το ίδιο, στην επιλογή του.

Όταν ένας χρήστης θελήσει να μπει σε ένα σύστημα, αυτό του ζητάει το username και το password του. Το Unix χρησιμοποιεί το αρχείο */etc/passwd*

όπου κρατάει στοιχεία για κάθε χρήστη που υπάρχει στο σύστημα. Το */etc/passwd* περιέχει το username, το πραγματικό όνομα, πληροφορίες αναγνώρισης όπως επίσης και βασικές πληροφορίες για το λογαριασμό του κάθε χρήστη. Τα πεδία που υπάρχουν σε κάθε γραμμή του αρχείου αυτού είναι το username, το κρυπτογραφημένο password του χρήστη, ο προσωπικός αριθμός αναγνώρισής του (UID), το group στο οποίο ανήκει ο χρήστης (GID), το πραγματικό όνομα του χρήστη, το home directory του και το shell του. Για παράδειγμα:

poco:dfgjfdhg/?hhg:156:100:Pole Cosis:/home3/popos:/bin/csh

Τα passwords αναπαρίστανται συνήθως με ένα ειδικό κρυπτογραφημένο format και μπορεί ακόμα και να μην είναι αποθηκευμένα σε αυτό το αρχείο αλλά σε ένα άλλο που λέγεται shadow και είναι ορατό μόνο από τον υπερ-χρήστη (superuser ή root).

Τα passwords είναι η πιο απλή μορφή πιστοποίησης της ταυτότητας κάποιου. Άλλες μορφές είναι η χρήση καρτών ή δακτυλικών αποτυπωμάτων οι οποίες όμως χρειάζονται ειδικό εξοπλισμό και είναι φυσικά πιο δαπανηρές αλλά και περιορίζονται σε ειδικές περιπτώσεις. Τα passwords είναι ένα μυστικό που μοιράζεται ο χρήστης με το υπολογιστικό σύστημα. Όταν μπαίνουμε στο σύστημα δίνουμε τον κωδικό μας ο οποίος συγκρίνεται από το σύστημα με αυτόν που αυτό έχει καταχωρημένο και εάν βρεθεί ίδιος τότε μας παρέχεται πρόσβαση. Το Unix δεν δείχνει τον κωδικό μας όταν τον πληκτρολογούμε και έτσι μας διασφαλίζει από την περίπτωση που κάποιος κοιτάει τι γράφουμε. Το password αποτελεί για το Unix την πρώτη γραμμή άμυνας στο σχεδιασμό ασφάλειάς του.

Το μειονέκτημα της χρήσης αυτών των συμβατικών κωδικών είναι το γεγονός ότι μπορούν πολύ εύκολα να υποκλεφτούν ειδικά εάν μπαίνουμε στο σύστημα από μακριά χρησιμοποιώντας το δίκτυο. Υπάρχουν πολλοί που με διάφορες μεθόδους μπορούν να αποκτήσουν τον προσωπικό μας κωδικό και να τον χρησιμοποιήσουν αργότερα για να προκαλέσουν ζημιά στο σύστημα, στα δεδομένα του ή για να αποκτήσουν πρόσβαση σε πληροφορίες που αλλιώς δεν θα μπορούσαν.

6.2.3 "Καλοί" και "Κακοί" Κωδικοί

Formatted ...
Formatted ...
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted ...
Formatted ...
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Right: 0,63 cm

Από την εμπειρία της διαχείρισης συστημάτων αλλά και από τα περιστατικά τα οποία βγαίνουν κάθε τόσο στην επιφάνεια και αφορούν την εύρεση κάποιου password ή την υποκλοπή του μπορούμε να θέσουμε κάποιες γενικές γραμμές επιλογής κωδικών. Τα καλά passwords ισοδυναμούν με κλειστές πόρτες για τους επίδοξους παραβιαστές ενός συστήματος ενώ αντίστοιχα τα passwords εκείνα που έχουν επιλεγεί με λανθασμένα κριτήρια ισοδυναμούν με πόρτες διάπλατα ανοικτές με τις ανάλογες επιπτώσεις.

Καλά passwords είναι αυτά που είναι δύσκολο να μαντέψει κανείς. Η συνταγή για την επιλογή ενός καλού κωδικού είναι :

- Να περιέχει τόσο κεφαλαία όσο και μικρά γράμματα
- Να περιέχει αριθμούς και σημεία στίξης
- Να περιέχει χαρακτήρες ελέγχου ή κενά
- Να είναι εύκολα στην απομνημόνευση έτσι ώστε να μην χρειάζεται να γραφτούν οπουδήποτε
- Να αποτελείται από 7-8 χαρακτήρες

Κακά passwords είναι εκείνα που αποτελούνται από:

- το όνομα του χρήστη
- από τα ονόματα συγγενικών του προσώπων
- γενικά από ονόματα
- το όνομα του λειτουργικού συστήματος
- το hostname του υπολογιστή
- τον αριθμό τηλεφώνου του χρήστη
- την ημερομηνία γέννησης κάποιου
- κάποια λέξη που αν και δυσεύρετη, ωστόσο περιέχεται στο λεξικό
- οτιδήποτε από τα παραπάνω το οποίο να έχει γραφεί ανάποδα

6.2.4 Το Σύστημα Αρχείων του Unix (UNIX Filesystem)

Το filesystem του Unix είναι αυτό που ελέγχει τον τρόπο με τον οποίο η πληροφορία που βρίσκεται σε αρχεία (files)και καταλόγους (directories) αποθηκεύεται στο σκληρό δίσκο και σε άλλες δευτερεύουσες μονάδες

Formatted: Font: (Default) Arial, Greek
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Bullets and Numbering
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Bullets and Numbering
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted: Font: (Default) Arial, 14 pt, Greek
Formatted: Font: (Default) Arial, 14 pt
Formatted ...
Formatted: Font: (Default) Arial, 14 pt
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Right: 0,63 cm

αποθήκευσης. Ελέγχει επιπλέον ποιοι χρήστες έχουν πρόσβαση, σε ποια αντικείμενα και πώς. Για αυτούς τους λόγους το σύστημα αρχείων είναι ένα από τα πιο σημαντικά εργαλεία στην υλοποίηση της ασφάλειας του Unix.

Αρχεία

Κάθε τι στο Unix αναπαρίσταται και εκπροσωπείται από κάποιο αρχείο είτε είναι κάποιο απλό αρχείο κειμένου είτε είναι κάποια συσκευή, διαδικασία ή δικτυακή σύνδεση.

Κατάλογοι

Οι κατάλογοι είναι ειδικά αρχεία του συστήματος αρχείων. Ο κατάλογος δεν είναι τίποτα περισσότερο από μια απλή λίστα ονομάτων και inode αριθμών (inode:για κάθε αντικείμενο του συστήματος αρχείων το Unix αποθηκεύει διαχειριστική πληροφορία στη δομή αυτή που υπάρχει στον δίσκο και δεν έχει όνομα αλλά μόνο αριθμό). Κάθε φυσιολογικός κατάλογος έχει πάντα δύο αρχεία. Το πρώτο είναι το ". " το οποίο σχετίζεται με το inode του ίδιου του καταλόγου και το ". . " το οποίο σχετίζεται με τον αμέσως πιο πάνω κατάλογο στη δομή των καταλόγων.

Ασφάλεια - Άδειες Χρήσης Αρχείων, Καταλόγων (File & Directory Permissions)

Η ασφάλεια αρχείων μας δίνει τη δυνατότητα να καθορίσουμε τι ακριβώς επιτρέπεται να κάνει κάποιος με τα αρχεία μας, δηλαδή αν μπορεί να τα διαβάσει, να τα αντιγράψει, να τα σβήσει ακόμα και να τα εκτελέσει. Αναλυτικά έχουμε τις τρεις παρακάτω επιλογές : read (r), write (w), execute (x).

Χαρακτήρας	Άδεια	Εξήγηση
r	Read—Διάβασμα	Μπορούμε να ανοίξουμε ένα αρχείο και να δούμε τα περιεχόμενά του
w	Write—Γράψιμο	Μπορούμε να αντιγράψουμε, να σβήσουμε ή να αλλάξουμε τα περιεχόμενα του

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Font: (Default) Arial
Formatted ...
Formatted: Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted ...
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted ...
Formatted: Right: 0,63 cm

		αρχείου
x	Execute—Εκτέλεση	Εάν το αρχείο είναι εκτελέσιμο τότε μπορούμε να το εκτελέσουμε πληκτρολογώντας το όνομά του

Ο αντίστοιχος πίνακας για τους καταλόγους είναι:

Περιεχόμενα	**Άδεια**	**Εξήγηση**
r	Read—Διάβασμα	Μπορούμε να δούμε ποια αρχεία βρίσκονται στον κατάλογο
w	Write—Γράψιμο	Μπορούμε να προσθέσουμε, να αφαιρέσουμε και να αλλάξουμε όνομα σε αρχεία του καταλόγου
x	Execute—Εκτέλεση	Μπορούμε να δούμε τους ιδιοκτήτες, τα μήκη και άλλα στοιχεία σχετικά με τα αρχεία που υπάρχουν σε ένα κατάλογο ή να πάμε σε αυτόν τον κατάλογο και να ανοίξουμε κάποια αρχεία σε αυτόν

Καταλαβαίνουμε λοιπόν, ότι οι άδειες που δίνουμε στα αρχεία μας όπως και στους καταλόγους αποτελούν ένα πολύ σημαντικό στοιχείο ασφάλειας και μας εξασφαλίζουν από πολλά. Σαν ιδιοκτήτες κάποιου αρχείου μπορούμε να θέσουμε όπως εμείς θέλουμε τις άδειες χρήσης του και να τις αλλάξουμε οποιαδήποτε στιγμή.

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

6.2.5 Λίστες Ελέγχου Πρόσβασης (Access Control Lists - ACLs)

Μερικές εκδόσεις του Unix υποστηρίζουν τις λίστες ελέγχου πρόσβασης ή ACLs. Αυτές παρέχονται συνήθως ως επέκταση των κανονικών αδειών χρήσης αρχείων που υπάρχουν στο Unix. Με τις ACLs μπορούμε να καθορίσουμε επιπλέον χαρακτηριστικά και δικαιώματα πρόσβασης για κάθε αρχείο και κατάλογο για πολλούς ξεχωριστούς χρήστες και επίσης να προσδώσουμε διαφορετικές άδειες σε μέλη διαφορετικών group. Αποτελούν ένα πολύ δυνατό χαρακτηριστικό του συστήματος και παρέχονται από τις εκδόσεις AIX και HP-UX του Unix ενώ υπάρχει πρόβλεψη να συμπεριληφθούν και σε μελλοντικές εκδόσεις των Solaris και Linux.

Τέλος πρέπει να πούμε ότι η ασφάλεια του Unix είναι ένα πολύ μεγάλο αντικείμενο το οποίο δεν μπορούμε να θεωρήσουμε ότι εξαντλείται σε λίγες γραμμές κειμένου. Ωστόσο, ότι αναφέρθηκε παραπάνω αποτελεί τη δομή γύρω από την οποία περιστρέφεται η ασφάλεια του Unix. Το λειτουργικό αυτό σύστημα είναι ότι πιο αξιόπιστο έχει δημιουργήσει, στον τομέα αυτό, ο άνθρωπος μέχρι σήμερα ενώ υπάρχουν στρατιές ολόκληρες δοκιμαστών και άλλων που συνεχώς εξελίσσουν όλα τα χαρακτηριστικά του συμπεριλαμβανομένης και της ασφάλειας που παρέχει στο μεμονωμένο χρήστη αλλά και στο δίκτυο σαν σύνολο.

6.3 Ασφάλεια και Java

Το περιβάλλον της Java παρέχει τη δυνατότητα εμφάνισης πληροφοριών “δυναμικού περιεχομένου” σε Hyper Text documents και σε εφαρμογές που εκτελούνται σε οποιαδήποτε πλατφόρμα (λειτουργικό σύστημα). Αυτό επιτυγχάνεται στο χώρο του Web μέσω των **applets** (προγράμματα γραμμένα σε Java, τα οποία ενσωματώνονται σε σελίδες HTML και μπορούν να εκτελούνται από όσους Web browsers υποστηρίζουν αυτήν τη δυνατότητα). Έτσι, η λειτουργικότητα της προάγει όλα εκείνα τα στοιχεία που συνθέτουν την εικόνα του μέλλοντος, όσον αφορά το Web και το Internet γενικότερα –

έξυπνοι πράκτορες, interactive 3D κόσμοι, self-updating λογισμικό και multimedia.

6.3.1 Λειτουργικότητα της Java.

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

- **Είναι μεταφέρσιμη.** Η Java μπορεί να τρέξει σε οποιονδήποτε υπολογιστή που διαθέτει Java interpreter. Αυτό σημαίνει ότι κάθε computer που θέλει να "τρέξει" Java, θα πρέπει να διαθέτει ένα πρόγραμμα που θα μετατρέψει τον Java κώδικα σε γλώσσα μηχανής. Εκτελούμενος σε interpreter περιβάλλον, ο Java κώδικας δεν χρειάζεται να προσαρμοστεί σε συγκεκριμένη hardware πλατφόρμα. Ο Java compiler που δημιουργεί τα εκτελέσιμα προγράμματα από πηγαίο κώδικα, μεταγλωττίζει για μια μηχανή που ουσιαστικά δεν υπάρχει.-η Java Virtual Machine (JVM). Η JVM είναι ένας (οποιοσδήποτε) υποθετικός επεξεργαστής που μπορεί να τρέξει Java κώδικα. Το παραδοσιακό πρόβλημα με τους interpreters, ήταν πάντα η έλλειψη ταχύτητας (performance). Η Java επιχειρεί να ξεπεράσει αυτό το πρόβλημα, μεταγλωττίζοντας σε ένα ενδιάμεσο στάδιο και μετατρέποντας τον Java κώδικα σε bytecode, ο οποίος έπειτα μετατρέπεται σε γλώσσα μηχανής για συγκεκριμένο επεξεργαστή.
- **Είναι "αυστηρή".** Οι δημιουργοί της Java, αρχικά επιχείρησαν να επεκτείνουν την C++, αλλά γρήγορα διαπίστωσαν ότι κάτι τέτοιο θα δημιουργούσε προβλήματα. Τα μεγαλύτερα εμπόδια του να καταστεί η

C++ μεταφέρσιμη, ήταν η χρήση δεικτών (pointers) για απευθείας διευθυνσιοδότηση της μνήμης, και η έλλειψη αυτόματης διαχείρισης της μνήμης. Αντίθετα, η Java δεν χρησιμοποιεί pointers και παρέχει αυτόματη διαχείριση μνήμης. Επειδή τα προγράμματα Java φορτώνονται και εκτελούνται αυτόματα, είναι ανεπίτρεπτο για μια εφαρμογή να έχει ένα bug που θα επιφέρει το "πέσιμο" (crash) του συστήματος, γράφοντας για παράδειγμα στη μνήμη του λειτουργικού συστήματος. Για αυτό το λόγο, η Java δε χρησιμοποιεί pointers. Η Java παρέχει αυτόματη διαχείριση μνήμης υπό τη μορφή "Αυτόματου συλλέκτη σκουπιδιών" (Automatic garbage collector). Ο garbage collector παρακολουθεί όλα τα αντικείμενα και τις αναφορές στα αντικείμενα, σε ένα πρόγραμμα Java. Όταν δεν υπάρχει αναφορά σε ένα αντικείμενο, ο garbage collector το "σταμπάρει" προορίζοντας το για απαλλαγή. Ο collector εκτελεί ένα thread (νήμα) χαμηλής προτεραιότητας στο background και "απαλλάσει" το αντικείμενο, ελευθερώνοντας μνήμη, είτε όταν το πρόγραμμα δεν χρησιμοποιεί πολλούς κύκλους επεξεργαστή (processor cycles), ή όταν υπάρχει ανάγκη για περισσότερη μνήμη. Εκτελώντας ένα ξεχωριστό thread, ο garbage collector παρέχει την ευκολία χρήσης και την αυστηρότητα ενός συστήματος αυτόματης διαχείρισης μνήμης, εξαλείφοντας το υπερφόρτωμα (overhead) που θα δημιουργούσε ένα full-time σχήμα διαχείρισης μνήμης.

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

-Bytecode verifier (πιστοποιητής bytecode)

-Runtime memory layout (runtime διάταξη μνήμης)

-Security manager (Διαχειριστής ασφαλείας)

- **Είναι αντικειμενοστρεαφής.** Έτσι, εξασφαλίζεται η επαναχρησιμοποίηση του κώδικα, η επεκτασιμότητά του και οι δυναμικές εφαρμογές που δημιουργούνται με αυτόν. Η **Τάξη** (Class) είναι μια συλλογή μεταβλητών και μεθόδων που ενθυλακώνει λειτουργικότητα σε ένα επαναχρησιμοποιήσιμο και δυναμικό αντικείμενο. Έτσι, αφότου δημιουργηθεί η Τάξη, μπορεί να χρησιμοποιηθεί ως template για τη δημιουργία επιπρόσθετων Τάξεων που παρέχουν επιπλέον λειτουργικότητα. Ένας προγραμματιστής για

Formatted ...

Formatted ...

Formatted: Font: (Default) Arial

Formatted: Indent: Left: 0,11 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted ...

Formatted: Bullets and Numbering

Formatted: Right: 0,63 cm

παράδειγμα, μπορεί να δημιουργήσει μια Τάξη για την εμφάνιση τετραγώνων στην οθόνη, και έπειτα να αποφασίσει ότι θα ήθελε να εμφανίζονται χρωματιστά τετράγωνα. Αντί να κατασκευάσει μια καινούρια Τάξη, ο προγραμματιστής μπορεί απλά να αναθέσει στην Java να χρησιμοποιήσει την παλιά Τάξη, με κάποια επιπλέον χαρακτηριστικά. Ουσιαστικά, ο χρήστης μπορεί να έχει το ίδιο αποτέλεσμα **χωρίς** να διαθέτειτον αρχικό πηγαίο κώδικα. Αφότου δημιουργηθεί μια Τάξη, το Java runtime περιβάλλον επιτρέπει το δυναμικό "φόρτωμα" Τάξεων. Αυτό σημαίνει ότι ήδη υπάρχουσες εφαρμογές μπορούν να αποκτήσουν περισσότερη λειτουργικότητα συνδεόμενες με Τάξεις που εμπεριέχουν τις απαραίτητες μεθόδους. Έτσι για παράδειγμα, ένας χρήστης που πλοηγείται στο Web βρίσκει ένα αρχείο για το οποίο δεν διαθέτει helper εφαρμογή. Χωρίς Java, ο χρήστης θα "κολλούσε" ψάχνωντας μια εφαρμογή που θα χειρίζονταν το αρχείο. Με Java, ο browser ζητάει από τον server μια Τάξη που μπορεί να χειριστεί το αρχείο, την "φορτώνει" δυναμικά μαζί με το αρχείο και το εμφανίζει χωρίς επιπλέον καθυστέρηση.

- **Είναι υψηλής απόδοσης.** Συνήθως το τίμημα της μεταφερσιμότητας, της ασφάλειας και της "αυστηρότητας", είναι η χαμηλή απόδοση. Είναι δύσκολο να πιστέψει κανείς ότι ο interpreted κώδικας μπορεί να "τρέχει" το ίδιο γρήγορα με τον κώδικα μηχανής.

Η Java, πάραυτα, χρησιμοποιεί ορισμένα tricks (κόλπα), που μειώνουν αρκετά το φόρτο λειτουργίας:

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

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

- **Just-in-Time Μεταγλωττιστής .** Ας υποθέσουμε ότι έχει γραφτεί ένας γρήγορος interpreter -στην C για παράδειγμα-. Αυτός διαθέτει ήδη μια χρήσιμη

ακολουθία binary κώδικα μηχανής, για κάθε bytecode που "μεταφράζει": *τον binary κώδικα που ο interpreter καθ'αυτός εκτελεί.* Επειδή ο interpreter έχει ήδη μεταγλωτιστεί από C σε binary κώδικα μηχανής, για κάθε bytecode που ερμηνεύει μετέρχεται σε μια ακολουθία οδηγιών (γλώσσας μηχανής) προς την hardware CPU στην οποία εκτελείται. "Σώζοντας" ένα αντίγραφο κάθε binary οδηγίας καθώς αυτή εκτελείται, ο interpreter μπορεί να διατηρεί έναν κατάλογο (log) του συνόλου των bytecodes που εκτελεί προκειμένου να "μεταφράσει" μια ολόκληρη μέθοδο. **Την επόμενη φορά που η μέθοδος εκτελείται,** ο interpreter απλά εκτελεί το αποθηκευμένο log του κώδικα μηχανής. Έτσι, η ταχύτητα είναι δέκα φορές μεγαλύτερη κατά μέσο όρο. Το trick αυτό, το ανακάλυψε ο Peter Deutsh προσπαθώντας να κάνει την Smaltalk να εκτελείται γρηγορότερα. Το ονόμασε "δυναμική μετάφραση". Η Sun το ονομάζει "just-in-time compiling".

6.3.2 Μηχανισμοί ασφαλείας της Java.

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

-Φόρτωμα του κώδικα

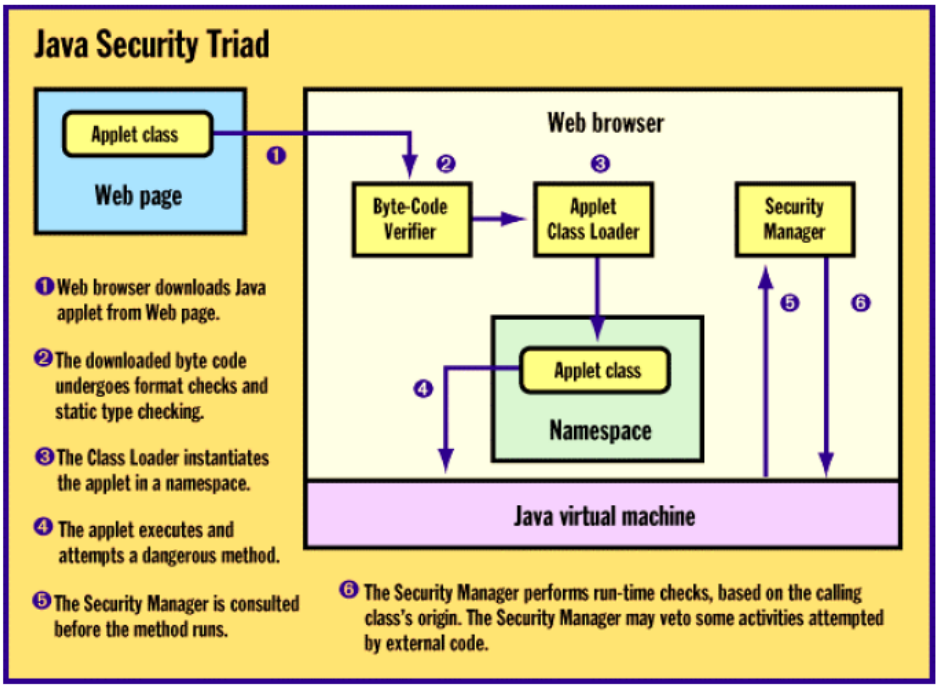
-Πιστοποίηση

-Εκτέλεση.

Η Τριάδα Ασφαλείας

Η ικανότητα της Java να "κατεβάσει" (download), να παράγει και να εκτελέσει

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



Σχημα1 Η Τριάδα Ασφαλείας της Java

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

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

Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines, Keep with next
Formatted: Font: (Default) Arial
Formatted: Caption, Line spacing: 1,5 lines, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Font: (Default) Arial, 11 pt, Not Bold
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Greek
Formatted: Font: (Default) Arial
Formatted: Bullets and Numbering
Formatted: Right: 0,63 cm

δυνατότητες (capabilities) επιτρέπουν “προχωρημένες” τεχνικές ασφαλείας για τα αρχεία I/O και την αυθεντικοποίηση.

- Ο δεύτερος μηχανισμός ασφαλείας, είναι ο **Applet Class Loader**. Όταν μια καινούρια Τάξη “φορτώνεται” στο σύστημα, αναγκαστικά θα προέρχεται από μια εκ των τριών περιοχών δραστηριοτήτων (realms): ο **τοπικός υπολογιστής**, το **τοπικό δίκτυο** (στο οποίο βρίσκεται ο υπολογιστής) που ενδεχομένως να βρίσκεται πίσω από firewall, το **Internet**. Κάθε μια από τις περιοχές αυτές τυγχάνει διαφορετικής μεταχείρισης από τον Class Loader. Συγκεκριμένα, ο Loader δεν επιτρέπει **ποτέ** μια Τάξη από μια “λιγότερο προστατευμένη” περιοχή να αντικαταστήσει μια τάξη από μια “περισσότερο προστατευμένη” περιοχή. Τα αρχεία συστήματος I/O για παράδειγμα, ορίζονται σε μια τοπική Java τάξη, δηλαδή ανήκουν στο realm “τοπικός υπολογιστής”. Έτσι, καμιά Τάξη έξω από τον υπολογιστή (είτε από το τοπικό δίκτυο, είτε από το Internet) δεν πρέπει να πάρει τη θέση κάποιας από αυτές τις Τάξεις. Επιπλέον, οι Τάξεις σε ένα realm δεν μπορούν να “καλέσουν” τις μεθόδους Τάξεων άλλων realms, εαν οι μέθοδοι δεν έχουν δηλωθεί public (δημόσιες) από τις Τάξεις. Επιπλέον, κάθε καινούριο applet που φορτώνεται από το δίκτυο, τοποθετείται σε ένα ξεχωριστό **namespace**. Τα namespaces επιτρέπουν την κατανομή των Java Τάξεων σε κατηγορίες, ανάλογα με το ποιά είναι η προέλευσή τους. Στην πραγματικότητα, ένα εκτελούμενο Java περιβάλλον μπορεί να διαθέτει πολλούς Class Loaders, καθ’ένας από τους οποίους καθορίζει το δικό του namespace. Με άλλα λόγια, κάθε Τάξη σχετίζεται με κάποιον Loader, ανάλογα με το από που προέρχεται. Κατ’ αυτόν τον τρόπο τα applets μπορούν να προστατεύονται και το ένα από το άλλο. Συνήθως, applets που προέρχονται από το ίδιο όνομα domain, ανήκουν στο ίδιο namespace. ~~Η φιλοσοφία των namespaces καθορίζεται (και) από την υλοποίηση του JDK (Java development Kit), του οποίου η τρέχουσα έκδοση είναι η 1.1.~~

- Ο τρίτος μηχανισμός ασφαλείας είναι ο **Security Manager** . *SecurityManager* είναι μια abstract (αφηρημένη) Τάξη η οποία έχει προστεθεί στο Java σύστημα. Μια πραγματοποίηση (instance) κάποιας

Formatted: Font: (Default) Arial, 12 pt
Formatted: Font: (Default) Arial
Formatted: Bullets and Numbering
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Bullets and Numbering
Formatted: Right: 0,63 cm

υποΤάξης της *SecurityManager* είναι ο τρέχων Security Manager. Έχει πλήρη έλεγχο σχετικά με το ποιές μέθοδοι, από ένα σύνολο ιδιαίτερα "επικίνδυνων" μεθόδων, επιτρέπεται να "καλούνται" από οποιαδήποτε δεδομένη Τάξη. Λαμβάνει υπ'όψην τα realms, την καταγωγή (προέλευση) της Τάξης και τον τύπο της Τάξης (αν είναι stand-alone ή "φορτωμένη" από ένα applet). Ποιό είναι όμως το σύνολο των "επικίνδυνων" μεθόδων που προστατεύονται; Τα αρχεία I/O είναι μέρος αυτού του συνόλου, για προφανείς λόγους. Επίσης, στο σύνολο "υπό προστασία" ανήκουν μέθοδοι που δημιουργούν και κάνουν χρήση συνδέσεων δικτύου, incoming (εισερχόμενων) ή outcoming (εξερχόμενων). Τέλος, σε αυτό το σύνολο ανήκουν οι μέθοδοι που επιτρέπουν σε ένα thread (νήμα) να έχει πρόσβαση, έλεγχο, δυνατότητα τροποποίησης άλλου νήματος.

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

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

απεριόριστη *(unrestricted)*: επιτρέπει στα applets να κάνουν ο,τιδήποτε.

firewall: επιτρέπει στα applets μέσα στο firewall να κάνουν ο,τιδήποτε.

πηγή *(source)*: επιτρέπει στα applets να κάνουν ο,τιδήποτε, στον host προορισμού τους, η με άλλο applet από εκεί.

τοπική *(local)*: Απαγορεύει εξολοκλήρου την πρόσβαση σε αρχεία και στο δίκτυο.

Formatted: Font: (Default) Arial, Bold

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Bold

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Bold

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Bold

Formatted: Font: (Default) Arial

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

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Ασφάλεια Τύπου

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Οι τρεις μηχανισμοί του μοντέλου ασφαλείας της Java, στους οποίους

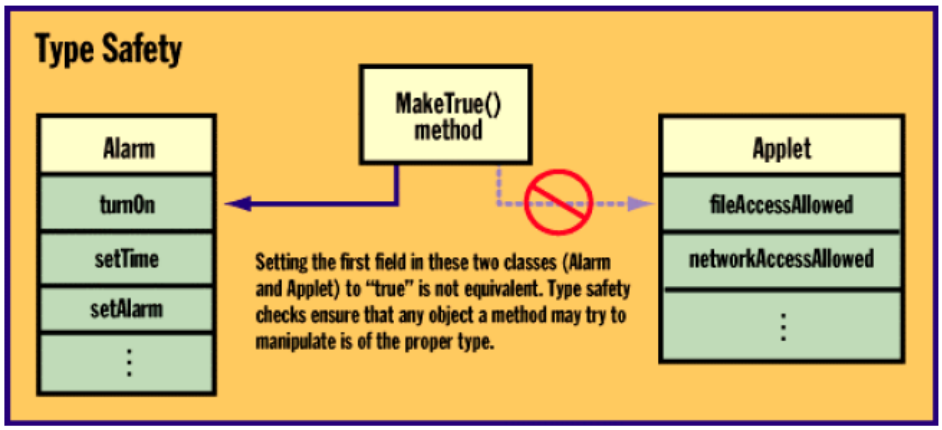
Formatted: Right: 0,63 cm

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

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

Ας υποθέσουμε τώρα ότι το πρόγραμμα επιχειρεί να εφαρμόσει τη *turnon* λειτουργία σε ένα Applet αντικείμενο. Εαν η *turnon* λειτουργία είναι επιτρεπτή, το πρόγραμμα καθιστά το πρώτο πεδίο του αντικειμένου αληθές (true). Δυστυχώς, εφόσον το αντικείμενο-στόχος είναι στην πραγματικότητα τύπου Applet, καθιστώντας το πρώτο πεδίο αληθές επιτρέπει την πρόσβαση του applet στο σύστημα αρχείων. Το applet έτσι---λανθασμένα—επιτρέπεται να τροποποιήσει ή ακόμα και να σβήσει αρχεία.

Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm



Σχήμα 2 Type Safety

Πώς η Java ενισχύει την Ασφάλεια τύπου

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

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

Υπάρχει εντούτοις ένα πρόβλημα με την στατική type-checking στρατηγική ~~της~~της Java: **είναι περίπλοκη**. Παρότι οι σχεδιαστές της Java συνέλαβαν ορθώς την

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines, Keep with next
Formatted: Caption, Line spacing: 1,5 lines, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

στρατηγική αυτή, υπάρχουν πολλές λεπτομέρειες που πρέπει να είναι σωστές

προκειμένου η Ασφάλεια Τύπου να είναι επιτυχής. Οποιοδήποτε λάθος σε κάποια από τις λεπτομέρειες, αφήνει μια μικρή αλλά ενδεχομένως σημαντική “τρύπα” στο σύστημα ασφαλείας. Ένας έξυπνος cracker που γίνεται γνώστης αυτής της “τρύπας” μπορεί να αρχίσει μια επίθεση *Σύγχισης Τύπου* (type-confusion attack). Ο cracker μπορεί να προκαλέσει μια κατάσταση παρόμοια με το Alarm/Applet παράδειγμα, όπου το πρόγραμμα έχει έναν τύπο αντικειμένου αλλά το σύστημα Java νομίζει ότι το αντικείμενο είναι άλλου τύπου.

Επειδή ο Verifier συνήθως αποτρέπει τέτοιες πράξεις, τα type-confusion λάθη

είναι συνήθως αποτέλεσμα λαθών (bugs) στην υλοποίηση του Java περιβάλλοντος.

6.3.3 Applets: Δικαιώματα και Υποχρεώσεις.

Ένα ιδιαίτερα “κομψό” αποτέλεσμα της ενσωματωμένης μεταφερσιμότητας ~~της~~της

Java είναι ότι ένα Java πρόγραμμα συγκεκριμένου είδους (γνωστό και ως applet) μπορεί να επισυναφθεί σε μια Web σελίδα . Τα applets ενσωματώνονται στον HTML κώδικα της Web σελίδας και “ερμηνεύονται” από Web browsers που έχουν αυτήν τη δυνατότητα. Σήμερα οι πιο δημοφιλείς browsers, ο Netscape Communicator και ο Microsoft Explorer αλλά και ο Hotjava της Sun “κατεβάζουν” (download) και αρχίζουν να εκτελούν οποιοδήποτε Java applet ανακαλύψουν ενσωματωμένο στην web σελίδα. Η Java, ως υλοποίηση της ιδέας του *“εκτελέσιμου περιεχομένου”*, παρέχει αυτήν τη δυνατότητα παράγοντας κώδικα ανεξάρτητα με την πλατφόρμα στην οποία αυτός θα εκτελεστεί. Υπάρχουν και άλλες ανταγωνιστικές υλοποιήσεις *“εκτελέσιμου περιεχομένου”*, όπως ActiveX, JavaScript, Safe-TCL, Telescript, Microsoft Word και Excel macros, και PostScript. Η Java όμως συνένωσε πολλούς κατασκευαστές λογισμικού “υπό την αιγίδα της” και αποτελεί την επικρατούσα τεχνολογία, τουλάχιστον προς το παρόν. **Ανεξάρτητα με την υλοποίηση πάντως, η εκτέλεση κώδικα άγνωστης -συνήθως- προέλευσης εγγυμονεί κινδύνους και προκαλεί ανασφάλεια στην κοινότητα των χρηστών του Web.** Τα applets μπορεί να γίνουν αρκετά

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, 14 pt, Underline

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, English (U.K.)

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, English (U.K.)

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, English (U.K.)

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, English (U.K.)

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, English (U.K.)

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, English (U.K.)

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, English (U.K.)

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, English (U.K.)

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

εχθρικά προς τον χρήστη, ανάλογα με τα δικαιώματα που τους παραχωρούνται, και τους περιορισμούς οι οποίοι τους επιβάλλονται.

Τα εχθρικά Applets διακρίνονται σε δύο κατηγορίες: Τα *"επιθετικά"* applets, τα

οποία μπορούν να προκαλέσουν σοβαρές παραβιάσεις στον τομέα της ασφάλειας, και τα *"πονηρά"* applets, τα οποία είναι περισσότερο ενοχλητικά παρά καταστροφικά .

Παρότι λιγότερο επώδυνα, τα "πονηρά" applets είναι ύπουλα, αφού μπορούν να

εκτελεστούν σε έναν υπολογιστή, με το που ο χρήστης του εισέλθει σε μια Web σελίδα.

Το Java run-time επιβάλλει περιορισμούς στο "τί μπορεί να κάνει ένα applet",

ανάλογα και με τη version του JDK, όπως θα δούμε και στη συνέχεια. Εντούτοις, ένα *"επιθετικό"* applet μπορεί να τροποποιήσει δεδομένα του σκληρού

δίσκου, να φανερώσει "μυστικά" δεδομένα σε τρίτους, να "μολύνει" έναν υπολογιστή με ιό (virus), να εγκαταστήσει ένα trapdoor. Ένας cracker μπορεί να επιτύχει τον απόλυτο έλεγχο του υπολογιστή του χρήστη-θύματος. Εως σήμερα, γνωρίζουμε οκτώ (8) σοβαρά προβλήματα ασφαλείας σε Java εφαρμογές, τα οποία ποικίλουν από προβλήματα στο DNS (Domain Naming System), εως type-confusion προβλήματα. Αυτές οι επιθέσεις δεν είναι υποθετικές. Κάθε επίθεση έχει υλοποιηθεί από την ομάδα Safe Internet Programming (SIP), γνωστή στην κοινότητα του Internet. Το σίγουρο είναι πως η κακόβουλη χρήση των applets προϋποθέτει βαθειά γνώση των περίπλοκων δομών της γλώσσας Java και του Internet. Εντούτοις, **ένα άτομο είναι αρκετό για να κατασκευάσει ένα εχθρικό applet**. Εφόσον αυτό συμβεί, η πληροφορία θα διαδοθεί μέσω της κοινότητας των crackers, και τα αποτελέσματα θα είναι καταστροφικά.

Ακόμα και το λιγότερο *"πονηρό"* applet μπορεί να "λεηλατήσει" τον ιδιωτικό βίο ενός χρήστη του Web. *"Πονηρά"* applets μπορούν να στέλνουν mails εκ μέρους του χρήστη-θύματος σε οποιονδήποτε λέγοντας ο,τιδήποτε, μπορούν να χρησιμοποιούν την ΚΜΕ (CPU) του υπολογιστή του θύματος για δικό τους λογαριασμό, "ρίχνοντας" έτσι το σύστημα του θύματος και απορροφώντας όλους τους υπολογιστικούς πόρους. Επίσης, *"πονηρά"* applets μπορεί να είναι ιδιαίτερα ενοχλητικά: εκτελούν αρχεία ήχου για πάντα,

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Font: (Default) Arial, Greek

Formatted: Font: (Default) Arial

Formatted: Right: 0,63 cm

καταγράφουν και παρακολουθούν (monitor) τις κινήσεις του χρήστη στο Web, εμφανίζουν στην οθόνη του ανεπιθύμητα γραφικά. Στο Web σήμερα είναι διαθέσιμες ολόκληρες συλλογές από *"πονηρά"* applets, για οποιονδήποτε ενδιαφερόμενο επιθυμεί να διαπιστώσει ιδίοις όμασι ποιά και πόσα applets αυτού του είδους υπάρχουν.

Προκειμένου να αντιμετωπίσει τα εχθρικά applets, η εταιρία JavaSoft αναζητεί

λύσεις που θα βελτιώσουν την εικόνα του συστήματος ασφαλείας στο Java Development Kit (JDK) με το οποίο εφοδιάζει τους χρήστες του Internet. Αξίζει να αναφέρουμε πως **στην πρώτη έκδοση του JDK (version 1.02)** τα applets δεν είχαν δικαίωμα ανάγνωσης, εγγραφής ή τροποποίησης δεδομένων σε τοπικά αποθηκευτικά μέσα του υπολογιστή που τα εκτελούσε. Έτσι, υπήρχε το λεγόμενο **"κουτί προστασίας"** (sandbox) – το ασφαλές browser partition όπου τα applets εκτελούνταν κανονικά. Στις 19 Φεβρουαρίου του 1997, η JavaSoft ανακοίνωσε την **έκδοση 1.1 του JDK** , στην οποία έκδοση υπάρχουν αρκετές καινοτομίες. Συγκεκριμένα, τα applets συνοδεύονται πλέον από την **ψηφιακή υπογραφή του δημιουργού τους**, η ταυτότητα του οποίου εμφανίζεται στον χρήστη που μετέρχεται στην Web σελίδα η οποία περιέχει το applet. Ο χρήστης καλείται να αποφασίσει εαν επιθυμεί την εκτέλεση του applet **πέρα από τα όρια του sandbox**, οπότε το applet πλέον **έχει δυνατότητες ανάγνωσης ή/και εγγραφής** στον σκληρό δίσκο του υπολογιστή του, ή μπορεί (το applet) να αποκτήσει πρόσβαση σε URL διαφορετικό από το δικό του. Το applet, στο JDK 1.1 θα τρέξει στα πλαίσια ασφαλείας του sanbox, εαν ο χρήστης δεν εμπιστεύεται τον υπογράφοντα. Η διαδικασία της υπογραφής, δεν είναι πανάκεια. Δεν εξαλείφει τα καταστροφικά αποτελέσματα στα οποία μπορέι να οδηγήσει η εκτέλεση ενός applet, απλά λέει στο χρήστη-θύμα ποιός είναι υπεύθυνος για την καταστροφή αυτή.

6.3.4 Java: ασφαλής, ή μήπως επικίνδυνη;

Στη συνέχεια, περιγράφουμε αναλυτικά τις κατηγορίες στις οποίες μπορούν να

ταξινομηθούν οι επιθέσεις με κακόβουλη χρήση της Java και των προγραμμάτων της, σε συνάρτηση πάντα με την υλοποίηση του Java runtime περιβάλλοντος αλλά και την

Formatted: Font: (Default) Arial, Not Bold
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

ανθεκτικότητα των browsers που την υποστηρίζουν .

6.3.5 Επιθέσεις Άρνησης Υπηρεσίας (denial of service attacks)

Η επιθέσεις αυτές συνιστούν την “εξάντληση” της ΚΜΕ και την δέσμευση μνήμης του υπολογιστή-θύματος, μέχρι την τελική κατάρρευσή του. Επιπλέον, ένα applet μπορεί να μπλοκάρει κρίσιμα “κομμάτια” του browser που το εκτελεί, καθιστώντας τον ανενεργό. Στον Netscape Navigator για παράδειγμα,η επίθεση αυτού του είδους μπορεί να “μποκάρει” την Τάξη java.net.InetAddress, μπλοκάροντας τις προσπάθειες του browser να αναζητήσει ονόματα hosts, με άλλα λόγια μπλοκάροντας όλες τις συνδέσεις δικτύου.

Υπάρχουν δύο λόγοι που καθιστούν τις **denial of service** επιθέσεις δύσκολο να

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

6.3.6 Πληροφορίες διαθέσιμες στα applets

Σε παλαιότερες εκδόσεις των browser HotJava (1.0) και Netscape Navigator (2.0), η κλήση συστήματος *accept ( )*, η οποία χρησιμοποιείται προκειμένου να δέχεται μία αίτηση για σύνδεση με κάποιον host, ύστερα από αίτηση του τελευταίου, δεν προστατεύονταν σωστά, με αποτέλεσμα κάποιο “κακόβουλο” applet **να ήταν ικανό να συνδεθεί με οποιονδήποτε browser, αρκεί να ήξερε τη διεύθυνσή του** –στις τελευταίες εκδόσεις των δύο browser η *accept* προστατεύεται καταλλήλως.

Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, 14 pt, Underline, English (U.K.)
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial, 14 pt, Underline, English (U.K.)
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial, 14 pt, Underline, English (U.K.)
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial, 14 pt, Underline, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 12 pt
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

Στον browser HotJava, για παράδειγμα (έκδοση 1.0) οι περισσότερες απόπειρες ενός applet να αναγνώσει ή να τροποποιήσει δεδομένα στο τοπικό σύστημα αρχείων, οδηγούν σε ένα dialog box το οποίο καλεί τον χρήστη να δώσει ή όχι τη συγκατάθεσή του. Ορισμένες Λίστες Ελέγχου Πρόσβασης (Access Control Lists) καθορίζουν πού μπορούν να πραγματοποιηθούν αναγνώσεις (read) ή/και εγγραφές (write) αρχείων ή καταλόγων χωρίς την συγκατάθεση του χρήση. Εξ' ορισμού, η write ACL είναι άδεια και η read ACL περιέχει τον κατάλογο (directory) στον οποίο βρίσκεται η βιβλιοθήκη του HotJava και συγκεκριμένα MIME mailcap αρχεία. Η read ACL επίσης περιέχει τον public_html κατάλογο του χρήστη, ο οποίος μπορεί να περιέχει κρίσιμες εμπιστευτικές πληροφορίες.

6.3.7 Λάθη Υλοποίησης (Implementation Errors)

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

DNS αδυναμίες

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

1) Πάρε όλες τις IP διευθύνσεις του hostname από το οποίο προήλθε το applet.

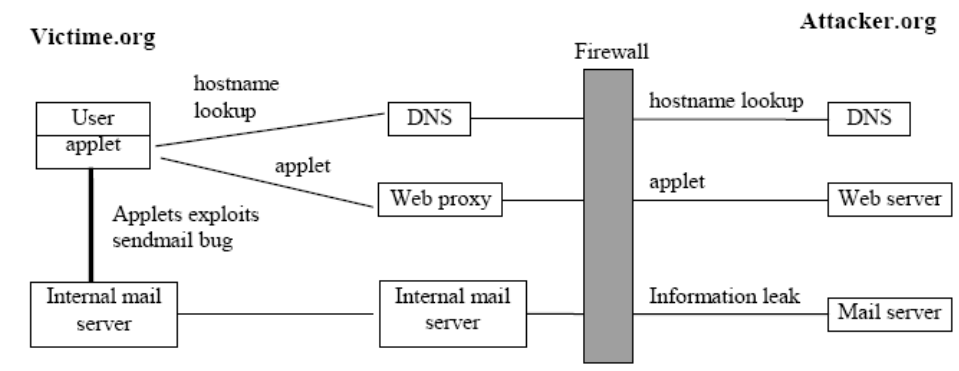
2) Πάρε όλες τις IP διευθύνσεις του hostname με το οποίο προσπαθεί να συνδεθεί το applet.

3) Εάν οποιαδήποτε διεύθυνση του πρώτου συνόλου ταυτίζεται με οποιαδήποτε διέθυνση του δευτέρου συνόλου, επέτρεψε τη σύνδεση. Ειδάλλως, εμπόδισε τη

Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

σύνδεση

Το πρόβλημα προκύπτει στο δεύτερο βήμα: το applet μπορεί να ζητήσει να συνδεθεί με οποιοδήποτε hostname στο Internet, επομένως μπορεί να γνωρίζει ποιός DNS server παρέχει τη δεύτερη λίστα των IP διευθύνσεων. Οι πληροφορίες από τον αναξιόπιστο αυτόν DNS server χρησιμοποιούνται στην απόφαση του συστήματος ασφαλείας. Όμως, **ένας "κακόβουλος" χρήστης ενδέχεται να κατασκευάσει έναν DNS server που ψεύδεται.** Συγκεκριμένα, μπορεί να ισχυριστεί (ο server) ότι το τάδε όνομα host (hostname) έχει τη δείνα IP διεύθυνση. Χρησιμοποιώντας τα ψευδή αυτά ζευγάρια διευθύνσεων (μηχανή-στην-οποία-συνδέομαι, μηχανή-από-την-οποία-προέρχομαι), ένα applet μπορεί να συνδεθεί με οποιονδήποτε υπολογιστή του Internet επιθυμεί. Αυτού του είδους οι επιθέσεις είναι πολύ επικίνδυνες, ιδιαίτερα όταν ο browser "τρέχει" πίσω από firewall, διότι το "κακόβουλο" applet μπορεί να προβεί σε επίθεση εναντίον οποιουδήποτε υπολογιστή βρίσκεται πίσω από το firewall. Μια τέτοια επίθεση φαίνεται στο σχήμα 3



Σχήμα 3 DNS Παράκαμψη Της Java

Όπως φαίνεται και στο σχήμα, ένα applet ταξιδεύει από το attacker.com στο victim.org μέσω νομίμων καναλιών. Το applet στη συνέχεια ζητάει να συνδεθεί στο

foo.attacker.com, ο οποίος σύμφωνα με τον ψευδή DNS server του attacker.com είναι ο εσωτερικός mail server του victim.org. Ο στόχος και τα αποτελέσματα της επίθεσης είναι προφανή.

Constructors ΥπερΤάξεων

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines, Keep with next
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Caption, Line spacing: 1,5 lines, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Right: 0,63 cm

Η γλώσσα Java δηλώνει ρητά ότι όλοι οι constructors, όταν πρωτο-
εκτελούνται
μπορούν να “καλέσουν” είτε κάποιον άλλο constructor της ιδίας Τάξης, ή
έναν
constructor υπερΤάξης. Οι Τάξεις συστήματος *ClassLoader, SecurityManager,* και
FileInputStream βασίζονται σε αυτήν τη συνθήκη για την ασφάλειά τους.
Αυτές οι
Τάξεις έχουν constructors οι οποίοι ελέγχουν εαν “καλούνται” από ένα
applet, και
οδηγούνται σε **SecurityException** εαν αυτό συμβαίνει. Δυστυχώς, ενώ ο
ακόλουθος
κώδικας δεν γίνεται δεκτός από την γλώσσα Java, ο bytecode Verifier
δέχεται το
ισοδύναμο bytecode του:

```
class CL extends ClassLoader {
        CL( ) {
                try { super( ); }
                catch (Exception e) { }
        }
}
```

Αυτός ο κώδικας επιτρέπει την κατασκευή ClassLoaders,
SecurityManagers, και
FileInputStreams. Ο ClassLoader είναι η πιο “ενδιαφέρουσα” Τάξη για
δειγματοποίηση, καθώς κάθε κώδικας που “φορτώνεται” από έναν
ClassLoader ρωτάει τον Classloader του προκειμένου να φορτώσει τις Τάξεις
που χρειάζεται. Ευτυχώς, από τη σκοπιά του “κακόβουλου” χρήστη, ο
κώδικας του constructor του ClassLoader **αρκεί να εκτελεστεί μία φορά**. Το
αποτέλεσμα αυτής της επίθεσης, τελικά, είναι **ένας ClassLoader υπό τον
έλεγχο του applet**. Εφόσον οι ClassLoaders καθορίζουν το namespace που
“βλέπουν” οι άλλες Τάξεις, **το applet πλέον μπορεί να κατασκευάσει ένα
αυθαίρετο namespace**.

Παράνομα Package ονόματα

Τα Java Packages (κάτι σαν τα Units στην Pascal) ονομάζονται συνήθως
java.io, *java.net*, κ.λ.π. Η java απαγορεύει ο χαρακτήρας ‘.’ να είναι ο πρώτος

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, English (U.K.)
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

χαρακτήρας του ονόματος του Package. Το runtime σύστημα αντικαθιστά κάθε '.' me '/' ώστε να προσαρμόσει την ιεραρχία των Packages στην ιεραρχία του συστήματος αρχείων. Ο μεταγλωττισμένος κώδικας αποθηκεύεται με τις τελείες να έχουν αντικατασταθεί με slashes. **Εαν ο πρώτος χαρακτήρας ενός ονόματος Package ήταν '/', το Java runtime σύστημα θα επιχειρούσε να φορτώσει κώδικα από ένα απόλυτο path** (μονοπάτι), εφόσον τα απόλυτα ονόματα path αρχίζουν με τον χαρακτήρα '/'. Έτσι, εαν ένας cracker μπορούσε να τοποθετήσει μεταγλωττισμένο κώδικα Java σε κάποιο αρχείο του συστήματος του "θύματος" (π.χ μέσω ενός κατανεμημένου συστήματος αρχείων, μέσω FTP κ.λ.π) **ο κώδικας του cracker θα θεωρούνταν "έμπιστος"**, αφού θα προέρχονταν από το τοπικό σύστημα αρχείων και όχι από το υπόλοιπο δίκτυο. Οι "έμπιστοι" κώδικες επιτρέπεται να φορτώνουν DLLs (Dynamic Link Libraries) τα οποία αγνοούν το Java runtime και **αποκτούν απευθείας πρόσβαση στο λειτουργικό σύστημα**, με όλα τα δικαιώματα του χρήστη-θύματος.

6.3.8 Σκέψεις για τη Java

Λάθος προσανατολισμός

Παρά την έξαρση που επικρατεί αυτήν τη στιγμή στους επιστημονικούς κύκλους σχετικά με την ασφάλεια στο Internet, και τον μεγάλο αριθμό βιβλίων και συγγραμμάτων που βλέπουν καθημερινά το φως της δημοσιότητας, η ουσία παραμένει η ίδια: Οι περισσότερες συζητήσεις και απόψεις δίνουν έμφαση σε κινδύνους οι οποίοι δεν έχουν υλοποιηθεί στην πράξη . Για παράδειγμα, η Java λέγεται ότι είναι ασφαλής επειδή τα Java applets δεν μπορούν να διαβάσουν ή να εγγράψουν σε αρχεία, στην client μηχανή (εκτός και υπάρχει άδεια για το αντίθετο, χάρη στο JDK 1.1).

Αλλά, σε μία από τις χαρακτηριστικότερες περιπτώσεις βανδαλισμού στο Internet, το Internet Worm τον Νοέμβριο του 1988, ούτε σβήστηκαν, ούτε τροποποιήθηκαν client αρχεία. Το πρόβλημα συνίστατο τότε στην "κλωνοποίηση" μονάδων του προγράμματος, που απομυζούσαν τους υπολογιστικούς πόρους μηχανών και καταλάμβαναν bandwidth σε τέτοιο σημείο που τα συστήματα κατέρρεαν.

Σε ένα κατανεμημένο σύστημα, συνήθως δεν παίζει τόσο μεγάλο ρόλο αν είναι

Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, 12 pt
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers
Formatted: Font: (Default) Arial, 14 pt, Underline
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

ασφαλής η πληροφορία, εκτός και αν δεν είναι δυνατή η παροχή της. Οι~~Η~~ επιθέσεις

Άρνησης Υπηρεσίας (Denial of Service) είναι πολύ αποτελεσματικές. Έτσι, όταν ένας~~ένας~~ υπολογιστικός πόρος εκτίθεται στο Internet, με τις επιθέσεις αυτού του είδους είναι δυνατός ο κορεσμός του σε τέτοιο σημείο ώστε οι νόμιμοι χρήστες να παύουν να εξυπηρετούνται.

Ουσιαστικά, ο κορεσμός υπολογιστικών πόρων είναι ίσως η μεγαλύτερη απειλή στην εμπορική βιωσιμότητα στο Internet.

Τα παιχνίδια που παίζουν οι άνθρωποι

Στο πανεπιστήμιο Hebrew της Ιερουσαλήμ και στο MIT Sloan School of Management, αντίστοιχα, οι ερευνητές Jeffrey Rosenschein και Gilad Zlotkin εξέτασαν τη χρήση τεχνικών θεωρίας παιγνίων στη μελέτη και πρόβλεψη αποτελεσμάτων.

Στο βιβλίο τους, “Rules of Encounter” (Mit Press), οι ερευνητές αυτοί τονίζουν δύο πτυχές σε οποιασδήποτε αλληλεπίδραση μεταξύ πρακτόρων. Η πρώτη, είναι “**Οι κανόνες του παιχνιδιού που ισχύουν για όλους**”, ανάλογοι με τα standards στο Internet όπως το Common Gateway Interface (CGI) και τη γλώσσα Java. Η δεύτερη, είναι η “**ξεχωριστή στρατηγική του κάθε συμμετέχοντα**”. Σε αυτό το σημείο, η Java δεν αποτελεί τίποτε περισσότερο από ένα δίκοπο μαχαίρι, όπως και κάθε τεχνολογία, δηλαδή δυνητικά τόσο χρήσιμη και καταστροφική όσο και οι προθέσεις του ατόμου που τη χρησιμοποιεί.

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

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

πραγματοποιήσουν τους στόχους τους με μη διαφανείς τρόπους.**Οι software πράκτορες δεν θα είναι περισσότερο αθώοι από τους ανθρώπους που τους δημιούργησαν**: "Δεν θα είναι εκ των προτέρων συνεργάσιμοι, ούτε θα μοιράζονται τις γνώσεις τους με άλλους, όπως και δεν θα υποχωρούν στο όνομα του "κοινού καλού," προειδοποιούν οι Rosenschein και Zlotkin.

Οι ευθύνες

Ένα άλλο θέμα το οποίο συγκεντρώνει μεγάλη προσοχή στις μέρες μας είναι αυτό της ασφάλειας σημαντικών δεδομένων όπως αριθμοί πιστωτικών καρτών. Έχουν προταθεί πολλά σχήματα –για παράδειγμα, η χρήση αλγορίθμων που αποδεικνύουν ότι το ένα απο τα συναλλασσόμενα μέρη κατέχει μια ποσότητα πληροφορίας χωρίς να την αποκαλύψει (αλγόριθμοι μηδενικής γνώσης). Αυτά τα σχήματα προφυλάσσουν τη συναλλαγή από **άτομα που δεν συμμετέχουν στη συναλλαγή**. Οι Υπεύθυνοι ασφαλείας δικτύων, που θεωρούν αυτά τα σχήματα ως επαρκή, αγνοούν συστηματικά τις "απάτες με πιστωτικές κάρτες" που γίνονται από τον έμπορο που συμμετέχει στη συναλλαγή. **Η συμμετοχή ενός προσώπου σε μια συναλλαγή, δεν σημαίνει ότι το πρόσωπο αυτό είναι έμπιστο**.

Άλλα δυνητικά προβλήματα, που είναι εξωγενή ως προς την Java, οφείλονται στις αλληλεπιδράσεις της με εργαλεία που την υποστηρίζουν, όπως οι Web browsers –οι οποίοι μπορεί να κάνουν χρήση cashing μηχανισμών, για παράδειγμα, που κατακρατούν σε ένα σχήμα ανασφαλή πληροφορία που θα έπρεπε να είναι ασφαλής.

Όπως και σε κάθε άλλη τεχνολογία επεξεργασίας πληροφορίας, η γνώση της Java για το σύστημα γύρω από αυτήν είναι περιορισμένη. **Οι Java εφαρμογές δεν έχουν την εγγενή δυνατότητα να συμπεράνουν ότι ένα συγκεκριμένο μήνυμα παρουσιάζει ενδιαφέρον για κάποιον**, πόσο μάλλον να επιτελέσουν συγκεκριμένες πράξεις ώστε να μην περιέλθει το μήνυμα σε αυτόν.

Εαν το λειτουργικό σύστημα ενός χρήστη καθιστά δυνατό μια διαδικασία να

Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Not Bold
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial, Greek
Formatted: Font: (Default) Arial
Formatted: Font: (Default) Arial
Formatted: Line spacing: 1,5 lines
Formatted: Font: (Default) Arial, Bold
Formatted: Font: (Default) Arial
Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines
Formatted: Font: (Default) Arial
Formatted: Right: 0,63 cm

εμπλακεί σε μια άλλη διαδικασία, η Java δεν μπορεί να το αποτρέψει αυτό. Δεν μπορεί για παράδειγμα να αποτρέψει ένα χρήστη ο οποίος θα ξεγελαστεί εκτελώντας μια utilty η οποία συγκεντρώνει και στέλνει ένα E-mail με αυτά που “μαθαίνει”.

Οι περισσότεροι σήμερα υϊοθετούν τη boolean λογική, μιλώντας για ασφαλείς ή

μη ασφαλείς τεχνολογίες. Όμως, υπάρχουν και άλλοι κρίκοι στην αλυσίδα που λέγεται “ασφάλεια ενός συστήματος”…

Formatted: Font: (Default) Arial

Formatted: Line spacing: 1,5 lines

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Βιβλιογραφία, πηγές

Από το διαδίκτυο:

- www.eos.gr
- www.lab.epmhs.gr
- http://thalis.cs.unipi.gr/~emagos
- http://alexandra.di.uoa.gr/mmtech

Formatted: Bullets and Numbering

Formatted: Right: 0,63 cm

- http://nemis.cti.gr/ebusiness
- http://pernet.teipir.gr/netlab
- http://aetos.it.teithe.gr/~vaf
- http://platon.teipir.gr/new/ecs
- www.ionio.gr
- www.e-yliko.sch.gr
- www.cineek.gr
- www.rsasecurity.com/rsalabs
- www.cryptogram.gr
- www.ebusinessforum.gr

Από βιβλία, περιοδικά:

- «Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο internet» του Douglas Comer
- «Ασφάλεια δικτύου» του Lincoln D. Stein
- Ελευθεροτυπία - 22/08/2005
- Pc magazine –Τεύχος Φεβρουαρίου- (θέμα:«Ασφάλεια, νέες απειλές, νέα αντιμετώπιση)

Formatted: Bullets and Numbering

Formatted: Greek

Formatted: Greek

Formatted: Font: (Default) Arial

Formatted: Indent: First line: 0,95 cm, Line spacing: 1,5 lines

Formatted: Line spacing: 1,5 lines

Formatted: Right: 0,63 cm