ΤΕΧΝΟΛΟΓΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΤΜΗΜΑ: ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ :

ΨΗΦΙΑΚΟ ΕΓΚΛΗΜΑ: ΒΑΘΥ ΚΑΙ ΣΚΟΤΕΙΝΟ ΔΙΚΤΥΟ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ : Τριανταφυλλάκης Γ. Αλέξανδρος
ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ: κ. Ασημακόπουλος Γεώργιος

ΝΟΕΜΒΡΙΟΣ 2016

ΕΥΧΑΡΙΣΤΙΕΣ

Ένα πολύ μεγάλο ευχαριστώ στον καθηγητή μου και επιβλέποντα της συγκεκριμένης πτυχιακής εργασίας κον Ασημακόπουλο Γεώργιο για την πολύ μεγάλη βοήθειά του κατά τη διάρκεια της έρευνάς μου.

Θα ήθελα επίσης να ευχαριστήσω όλους τους ειδικούς αλλά και εκείνους που ασχολούνται με την μελέτη του σκοτεινού διαδικτύου, τη λογική του Darknet που παρέχει ανωνυμία σε όσους το χρησιμοποιούν – κάτι που, όπως ισχύει και στον πραγματικό κόσμο, και αποτελεί μια ευκαιρία την οποία δεν αφήνουν ανεκμετάλλευτη οι εγκληματίες.

Τέλος , θα επιθυμούσα να αποστείλω τις ευχαριστίες μου στα μέλη της οικογένειάς μου αλλά και στους φίλους μου, οι οποίοι όλο αυτόν τον καιρό της προετοιμασίας της συγκεκριμένης εργασίας αλλά και έρευνας με στήριξαν σε υπέρτατο βαθμό.

ΠΡΟΛΟΓΟΣ

Από τους εκατομμύρια ανθρώπους που «σερφάρουν» καθημερινά από τον υπολογιστή ή την «έξυπνη» συσκευή τους, πολλοί ίσως δεν έχουν διανοηθεί πως, εκτός από το «ορατό» Ιντερνετ, υπάρχει κι ένα παράλληλο online «σύμπαν» από υπηρεσίες και ιστοσελίδες στις οποίες δεν υπάρχει περίπτωση να... πέσουν κατά τύχη πάνω τους. Απροσπέλαστο από τους συμβατικούς browser, το «σύμπαν» αυτό έχει «βαφτισθεί» Σκοτεινό Διαδίκτυο (Darknet). Ενα όνομα που χρωστά στο γεγονός ότι παραμένει κρυμμένο από τις μηχανές αναζήτησης που «σαρώνουν» το web, όπως και από τις διωκτικές αρχές ή τις υπόλοιπες κρατικές υπηρεσίες ανά τον κόσμο.

Η λογική του Darknet είναι να παρέχει ανωνυμία σε όσους το χρησιμοποιούν – κάτι που, όπως ισχύει και στον πραγματικό κόσμο, αποτελεί μια ευκαιρία την οποία δεν θα άφηναν ανεκμετάλλευτη οι εγκληματίες. Από τις έκνομες δραστηριότητες που έχουν βρει «στέγη» σε αυτό, ψηλά στη λίστα βρίσκεται η διακίνηση κάθε λογής παράνομου προϊόντος ή υλικού. Ετσι, το Σκοτεινό Διαδίκτυο επιστρατεύεται κατά κόρον για αγοραπωλησίες παιδικής πορνογραφίας, ναρκωτικών, όπλων, κλεμμένων πιστωτικών καρτών και πλαστών ταυτοτήτων.

Στις περισσότερες περιπτώσεις, οι παράνομες συναλλαγές γίνονται από online «μαύρες αγορές», δηλαδή σάιτ όπου οι «πωλητές» αναρτούν τις αγγελίες τους και δέχονται παραγγελίες. Οπως λειτουργεί και το νόμιμο ηλεκτρονικό εμπόριο, τα προϊόντα αποστέλλονται ταχυδρομικά, στη διεύθυνση που θα επιλέξει ο αγοραστής. Με τη διαφορά ότι οι αγοραπωλησίες γίνονται ως επί το πλείστον σε bitcoin, το εικονικό νόμισμα στο οποίο δεν εμπλέκεται κάποια κεντρική τράπεζα, με συνέπεια να είναι πιο δύσκολο να ανιχνευθούν οι συναλλαγές.

Το Darknet είναι ένα δίκτυο από σέρβερ, οι οποίοι βασίζονται σε τεχνολογίες κρυπτογράφησης για να ανταλλάσσουν δεδομένα. Η πιο διαδεδομένη τεχνολογία γι' αυτό τον σκοπό είναι το Tor (The onion router), το οποίο αναπτύχθηκε αρχικά από το Ερευνητικό Εργαστήριο του αμερικανικού πολεμικού ναυτικού, για την προστασία των στρατιωτικών επικοινωνιών. Χάρις στο Tor, ένα σάιτ μπορεί να αποκρύπτει τα ψηφιακά του ίχνη, «καμουφλάροντας» τον σέρβερ που το φιλοξενεί. Παράλληλα, η τεχνολογία εξασφαλίζει πως πρόσβαση στο Σκοτεινό Διαδίκτυο έχουν μόνον χρήστες που έχουν εγκαταστήσει το ανάλογο λογισμικό στο μηχάνημά τους. Λογισμικό που εγγυάται και τη δική τους ανωνυμία.

Μέχρι πρόσφατα, ακόμη κι αν είχε κανείς εγκαταστήσει το software, θα έπρεπε να γνωρίζει επίσης τη συγκεκριμένη διεύθυνση κάθε ιστοσελίδας που θέλει να επισκεφθεί. Ωστόσο, πριν από λίγες εβδομάδες, το Darknet απέκτησε το δικό του «ψαχτήρι», το Grams, μια μηχανή αναζήτησης που συγκεντρώνει αποτελέσματα από οκτώ online «μαύρες αγορές» και τις αγγελίες τους. Βέβαια, το κίνητρο του

δημιουργού του Grams είναι το κέρδος, αφού όπως ανέφερε στο αμερικανικό περιοδικό Wired, σύντομα θα αρχίσει να χρεώνει όσους θέλουν οι αγγελίες τους να εμφανίζονται ψηλότερα στα αποτελέσματα.

Εξάλλου, το κέρδος είναι επίσης βασική αιτία που οι περισσότερες από αυτές τις ιστοσελίδες εμφανίστηκαν μετά τον περασμένο Οκτώβριο και παρά τη σύλληψη τότε από το FBI του ανθρώπου που φέρεται να είναι ο «εγκέφαλος» πίσω από το Silk Road, -«μια από τις πιο εξελιγμένες online “μαύρες αγορές”» όπως έχει χαρακτηρισθεί. Κι αυτό γιατί, με βάση τη δικογραφία, τα έσοδα του Silk Road μέσα σε λιγότερο από 3 χρόνια λειτουργίας άγγιξαν τα 80 εκατομμύρια δολάρια, από την προμήθεια που χρέωνε για κάθε αγοραπωλησία. Μάλιστα, οι συναλλαγές που έγιναν στο διάστημα λειτουργίας του σάιτ φαίνεται πως ξεπέρασαν τα 1,2 δισ. δολ.

Πάντως, σύμφωνα με τις διωκτικές αρχές σε όλο τον κόσμο, το Σκοτεινό Διαδίκτυο κάνει πιο δύσκολη την αντιμετώπιση του online εγκλήματος, όχι όμως και αδύνατη. Ετσι, ενώ ο κατηγορούμενος ως διαχειριστής του Silk Road περιμένει να δικασθεί, αντιμετωπίζοντας ποινή φυλάκισης τουλάχιστον 30 ετών, τον Φεβρουάριο εξαρθρώθηκε μια ακόμη online «μαύρη αγορά», η Utopia, με τη σύλληψη πέντε υπόπτων από την ολλανδική και τη γερμανική αστυνομία.

Πάγια τακτική είναι οι αρχές να μην αποκαλύπτουν τι είδους ηλεκτρονικά «αντίμετρα» επιστρατεύουν – στην περίπτωση του Silk Road, ο εκπρόσωπος του FBI αναφέρθηκε απλώς σε «ανθρώπινα λάθη» που οδήγησαν στα ίχνη του διαχειριστή του. Από την άλλη μεριά, οι αρχές εκμεταλλεύονται το γεγονός ότι τα εγκλήματα στον online κόσμο αφήνουν ίχνη και στον πραγματικό: για την εξάρθρωση του Utopia, σύμφωνα με το δελτίο Τύπου της ολλανδικής αστυνομίας, αστυνομικοί υποδύθηκαν τους «πελάτες», αγοράζοντας ναρκωτικά και όπλα. «Η επιχείρηση στέλνει ένα ξεκάθαρο μήνυμα πως κανείς δεν μπορεί να ξεγλιστρήσει, επειδή χρησιμοποιεί το Tor», αναφέρεται χαρακτηριστικά στην ανακοίνωση.

Η φωτεινή πλευρά

Μπορεί το Darknet να έρχεται στην επικαιρότητα συνήθως με αφορμή αστυνομικές επιχειρήσεις που έχουν στο στόχαστρο «μαύρες αγορές» σαν το Silk Road, ωστόσο αυτό δεν σημαίνει πως είναι απλώς το online ανάλογο του πραγματικού υποκόσμου. «Το Σκοτεινό Διαδίκτυο έχει και μία εξαιρετικά σημαντική “φωτεινή” πλευρά, εξασφαλίζοντας την ελευθερία της έκφρασης σε ανθρώπους που ζουν σε απολυταρχικά καθεστώτα και βοηθώντας να έρθουν στο φως συνταρακτικά ντοκουμέντα, χωρίς τον φόβο όσων τα διέρρευσαν πως θα διωχθούν ποινικά», σημειώνει ο Brad Chacos από το περιοδικό PC World.

Ενδεικτικά, στο Darknet έχουν κατά καιρούς φιλοξενηθεί αντίγραφα του GlobalLeaks και του Wikileaks, ενώ το περιοδικό New Yorker έχει δημιουργήσει το Strongbox, μια υπηρεσία στο Σκοτεινό Διαδίκτυο που εγγυάται ανωνυμία σε όσους θελήσουν να

επικοινωνήσουν με τους συντάκτες του με μεγαλύτερη ασφάλεια από αυτήν που προσφέρουν τα ηλεκτρονικά ταχυδρομεία. Επίσης, η οργάνωση «Δημοσιογράφοι Χωρίς Σύνορα» συμβουλεύει τα μέλη της να το χρησιμοποιούν για να έρχονται σε επαφή με τις πηγές τους, στην περίπτωση που θέλουν να διασφαλίσουν πως θα μείνει μυστική η ταυτότητα όσων επικοινωνούν.

Παράλληλα, σε εργαλεία και υπηρεσίες που βασίζονται στο Tor βρίσκουν «καταφύγιο» απλοί χρήστες που θέλουν να παρακάμψουν τα «φίλτρα» ιντερνετικής λογοκρισίας στη χώρα τους και, όπως είναι φυσικό, πολιτικοί ακτιβιστές. Ετσι, σύμφωνα με την ιστοσελίδα του The Tor Project, το Darknet κατακλύσθηκε από μπλογκ κατά τη διάρκεια της «Αραβικής Ανοιξης», από ανθρώπους που συμμετείχαν στις εξεγέρσεις και ήθελαν να μεταφέρουν στο εξωτερικό τη μαρτυρία τους. Δυνατότητες που, όπως σημειώνει ο συντάκτης του PC World, δεν θα μπορούσαν να γίνουν πραγματικότητα, αν το Σκοτεινό Διαδίκτυο δεν προσέφερε ένα επίπεδο ασφάλειας το οποίο δυστυχώς το κάνει ελκυστικό και σε εγκληματίες.

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία χωρίζεται σε τέσσερα μέρη.

1ο ΜΕΡΟΣ

Στο ΚΕΦΑΛΑΙΟ 1 ορίζεται η έννοια του εγκλήματος,του διαδικτύου ,τα χαρακτηριστικά γνωρίσματα των εγκλημάτων στον κυβερνοχώρο και τα χαρακτηριστικά του ψηφιακού εγκληματία.

Στο ΚΕΦΑΛΑΙΟ 2 αναλύονται τα γνήσια ηλεκτρονικά εγκλήματα και τα συμβατικά εγκλήματα που τελούνται με χρήση Η/Υ και διαδικτύου.

2ο ΜΕΡΟΣ

Το ΚΕΦΑΛΑΙΟ 3 στην ασφαλή χρήση του διαδικτύου , τη χρήση λογισμικών ασφαλείας και στα συστήματα ανίχνευσης επιθέσεων μεσω διαδικτύου.

Στο ΚΕΦΑΛΑΙΟ 4 αναλύονται οι πολιτικές ασφαλείας των WEB εξυπηρετών και WEB εφαρμογών.

3ο ΜΕΡΟΣ

Στο ΚΕΦΑΛΑΙΟ 5 αναλύεται η έννοια της κρυπτογράφησης και η αποδεικνύεται η αναγκαιοτητά της για διαδικτυακή ασφάλεια.

Στο ΚΕΦΑΛΑΙΟ 6 αναλύονται τα δημάσια κλειδιά ,τα ψηφιακά πιστοποιητικά, η διαχείρηση κλειδιών και πιστοποιητικών και η αρχιτεκτονική υποδομή δημοσίου κλειδιού.

Στο ΚΕΦΑΛΑΙΟ 7 αναλύονται οι ψηφιακές υπογραφές.

4ο ΜΕΡΟΣ

Στο ΚΕΦΑΛΑΙΟ 8 γίνεται αναφορά στο TOR (The Onion Router) ,στη λειτουργία του δικτύου και στις αδυναμίες του.

Το ΚΕΦΑΛΑΙΟ 9 αναφέρεται στους τρόπους περιορισμού της χρήσης των προσωπικών δεδομένων στο διαδίκτυο.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 4

ΜΕΡΟΣ 1ο

Εισαγωγή

Η πληροφορική, οι υπολογιστές, το διαδίκτυο και γενικότερα η σύγχρονη τεχνολογία έχου εισβάλει στην καθημερινότητα του ανθρώπου, καθώς του παρέχουν μια σειρά δυνατοτήτων που βελτιώνουν την ποιότητα της ζωής του.Η απλοποίηση κάποιων εργασιών, η οργάνωση των πληροφοριών, η επιτάχυνση διαδικασιών όπως και ο ακριβής, άμεσος υπολογισμός και διαχείρηση μεγάλου όγκου δεδομένων είναι λίγες μόνο από τις ωφέλειες που μπορεί να καρπωθεί ο σύγχρονος άνθρωπος από τη ραγδαίως αναπτυσσόμενη πληροφορική τεχνολογία.
Το διαδίκτυο αποτελεί το μεγαλύτερο υπολογιστικό σύστημα στον κόσμο. Η εξελιξή του βασίστηκε στη φιλοσοφία ενός έκκεντρου, ανοιχτού συστήματος χωρίς ιδιαίτερο έλεγχο από κάποια ερχή και αυτό γιατί το διαδίκτυο δεν είναι ιδιοκτησία κανενός. Παρόλα αυτά όμως μπορεί να γίνει εύκολα αντιληπτό, πως λόγω του παλλαπλασιασμού των χρηστών, κρίνεται πλέον αναγκαία η οργάνωση καθώς και ο έλεγχός του, ώστε να εξασφαλίζεται η σωστή λειτουργία του.Μπορούμε να το φανταστούμε ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, που συνδέει εκατομμύρια υπολογιστών σε χιλιάδες δίκτυα διασκορπισμένα ανά τον κόσμο, παρέχοντας στους χρήστες τους μια τεράστια ποικιλία εργαλείων και υπηρεσιών.
Από την άλλη, ένα από τα πλέον αρνητικά στοιχεία της πληροφορικής τεχνολογίας, είναι η δημιουργία πρόσφορωνσυνθηκών για την ανάπτυξη και διάδοση νέων μορφών εγκλημάτων.Το ηλεκτρονικό έγκλημα είναι ένα φαινόμενο εξελισσόμενο με ταχύτατους ρυθμούς, καθώς συμβαδίζει με αυτούς της ανάπτυξης της τεχνολογίας.Υπάρχει επομένως κίνδυνος κάθε είδους απάτης, από καλούς γνώστες της τεχνολογίας, οι οποίοι προσπαθούν να πραγματοποιήσουν παράνομες πράξεις, μετατρέποντας την τεχνολογία κατά αυτόν τον τρόπο σε ένα καταστροφικό όπλο. Οι δυνατότητες δίωξης από τις αρμόδιες αρχές είναι περιορισμένες, καθώς υπάρχει έλλειψη εμπειρίας αλλά και εκπαίδευσης σε επαρκή βαθμό όπως επίσης και ασάφεια όσον αφορά τη νομοθεσία.

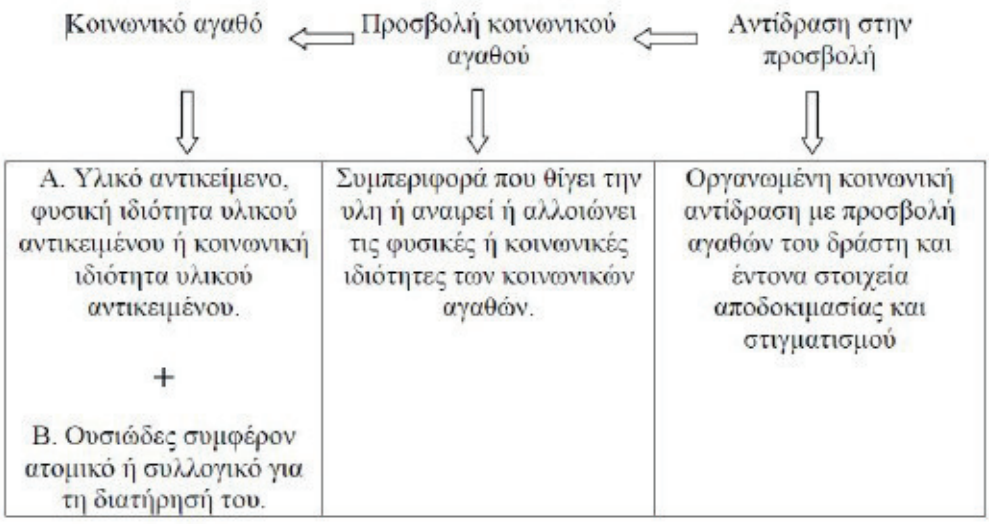
ΚΕΦΑΛΑΙΟ 1

Σε αυτό το κεφάλαιο θα αναλυθεί εν συντομία το εγκληματικό φαινόμενο στη συμβατική του αρχικά μορφή. Στη συνέχεια θα αναφερθούμε στην έννοια του Διαδικτύου και πως η είσοδος του στην καθημερινότητα μας έχει φέρει τεράστιες αλλαγές. Η χρήση του Διαδικτύου στην Ελλάδα, μέσα από επίσημα, πρόσφατα στοιχεία.Τέλος αναφορά γίνεται στη νέα μορφή παραβατικής συμπεριφοράς που καλείται ηλεκτρονικόή αλλιώς ψηφιακόέγκλημα. Παρατίθενται ιστορικά στοιχεία καθώς και τα κυριότερα χαρακτηριστικά του.

1.1 ΕΓΚΛΗΜΑ

Το έγκλημα είναι αναπόσπαστο κομμάτι κάθε κοινωνίας και συμπεριφέρεται σαν ένας ζωντανός οργανισμός που διαρκώς μεταβάλλονται οι μορφές, τα μέσα διάπραξης καθώς και η νομοθεσία που το διέπει.Με διαφορετικό περιτύλιγμα αλλά και ουσία πολλές φορές, ανάλογα με τις πολιτικές, κοινωνικές και ηθικές τάσεις κάθε εποχής έγκλημα παραμένει παρόν, κινούμενο πάντα σε τρείς βασικούς άξονες, τα απαραίτητα συστατικά στοιχεία του, αυτά που το ορίζουν.Ποιά είναι όμως αυτά τα στοιχεία; Το εγκληματικό φαινόμενο εμφανίζεται στον κοινωνικό χώρο ως σύνθεση των παρακάτω στοιχείων που φαίνονται στον πίνακα:

Πίνακας 1.1: Βασικά στοιχεία του εγκλήματος



Το εγκληματικό φαινόμενο αποτελεί ιστορικό, κοινωνικό φαινόμενο, καθώς

ακολουθεί την εξέλιξη των ανθρώπινων κοινωνιών. Έτσι τα επιμέρους χαρακτηριστικά του, (κοινωνικά αγαθά, έγκλημα, ποινή) έχουν και αυτά ιστορικότητα, δηλαδή σχετικότητα, διαφοροποιούμενα από τόπο σε τόπο και από εποχή σε εποχή. Αυτό που έχει ιδιαίτερη σημασία να επισημάνουμε σχετικά με το εγκληματικό φαινόμενο είναι η διαχρονικότητά του στο πέρασμα των αιώνων. Αν και σε κάθε έγκλημα (προσβολή) , υπήρχε, υπάρχει και θα υπάρχει ποινή (αντίδραση), απεναντίας καμμία κοινωνία δεν έχει απαλλαχθεί από αυτό. Αυτό που παρατηρείται είναι μια συνεχής αύξηση του εγκληματικού φαινομένου και συγχρόνως εμφάνιση νέων μορφών εγκληματικής συμπεριφοράς.
Υπάρχουν άνθρωποι οι οποίοι παραβαίνουν τους κοινωνικούς κανόνες,ναυτούς που θεσπίστηκαν τυπικά ή άτυπα προκειμένου να διαφυλαχθούν τα κοινωνικά αγαθά. Αποτέλεσμα της προσβολής αυτών των αγαθών είναι η επιβολή διαφόρων κυρώσεων στους παραβάτες. Η επιβληθείσα κύρωση ή αλλιών ποινή, θα μπορούσαμε να πούμε ότι αποτελεί τον τρόπο αντίδρασης της κοινωνίας στο έγκλημα. Η αντίδραση, καθώς και το είδος της ποινής, απευθύνεται στον παραβάτη των κοινωνικών κανόνων και βρίσκονται πάντα σε στενή εξάρτηση με την εκάστοτε εποχή και πολιτισμό.

Το έγκλημα είναι αναμενόμενο στα πλαίσια της κοινωνικής πραγματικότητας.Είναι το εμφανές σύμπτωμα της κοινωνικής κρίσης, της διάρρηξης του κοινωνικού ιστού, το βαθύ σημάδι μιας κοινωνίας που γερνά. Όπως αναφέρθηκε και παραπάνω, υπάρχουν οι κανόνες για να ρυθμίζουν την ομαλή συμβίωση των μελών μιας οργανωμένης κοινωνίας. Είναι αδύνατον όμως όλα τα μέλη να συμμορφώνονται με τους ίδιους κανόνες, καθώς η τήρησή τους είνα στενά συνδεδεμένη και με τη διαφορετική προσωπικότητα του κάθε ατόμου.
Τα βασικά στοιχεία του εγκληματικού φαινομένου, κανόνας, έγκλημα, κύρωση, συναποτελούν έναν αδιάσπαστο κύκλο. Εδώ είναι ξεκάθαρη η αλληλεξάρτηση των στοιχείων. Αν δεν υπήρχε έγκλημα δεν θα υφίστατο η κύρωση. Η μη ύπαρξη κανόνα δεν καθιστά δυνατή τηνπαράβασή του. Ο κανόνας δημιουργήθηκε για να οργανώσει και να προστατεύσειντα κοινωνικά αγαθά (υλικά και άυλα) από κάθε προσβολή τους μέσα στα πλάισια της κοινωνικής συμβίωσης. Στη συνέχεια, και αφού επέλθει η προσβολή του έννομου αγαθού (αυτό που προστατεύεται από τον κανόνα-νόμο), έρχεται η κύρωση (ποινή). Είναι με λίγα λόγια η κύρωση συνέπεια της παράβασης του κανόνα και δηλώνει προς αυτόν που επιβάλλεται ότι η συγκεκριμένη συμπεριφορά δεν είναι αποδεκτή από την κοινωνία. Θα λέγαμε ότι η ποινή αποτελεί την εκτόνωση της κοινωνικής αντίδρασης στο έγκλημα. Μπορεί δε, να παρουσιαστεί με πολλούς διαφορετικούς τρόπους, όσο αφορά την ιδεολογική της προσέγγιση, όπως ως αποκατάσταση της διαταχθείσας από το έγκλημα κοινωνικής τάξης ή ως το μέσο για την ηθική βελτίωση του παραβάτη.

1.2 ΔΙΑΔΙΚΤΥΟ

Το διαδίκτυο (ίντερνετ) μπορεί να πριγραφεί ως ένα τεράστιο πλέγμα ψηφιακών γραμμών, το οποίο διασυνδέει εκατομμύρια υπολογιστών σε χιλάδες δίκτυα, διασκορπισμένα σε ολόκληρο τον κόσμο, παρέχοντας σε αυτούς ποικιλία υπηρεσιών

και εργαλείων. Είναι ένας απέραντος εικονικός κόσμος στον οποίο μπορεί εύκολα να έχουν πρόσβαση χρήστες κάθε ηλικίας. Με τη σημερινή του μορφή (World Wide Web-www), εισέβαλε στη ζωή μας πριν από 29 περίπου χρόνια, αλλάζοντας ριζικά την πλειοψηφία των ανθρώπινων δραστηριοτήτων.

Το διαδίκτυο και κατ΄επέκταση οι ηλεκτρονικοί υπολογιστές (Η/Υ), έχουν καταστεί αναπόσπαστα κομμάτια της καθημερινότητάς μας, είτε ως μέσα ψυχαγωγίας, ενημέρωσης, είτε, το πιο σημαντικό, ως εργαλεία πληροφόρησης και διεκπεραίωσης επαγγελματικών υποχρεώσεων και δραστηριοτήτων.
Η πληροφορία στην εποχή του διαδικτύου έχει αποκτήσει τη θέση ενός αυτόνομου αγαθού. Οι ποσότητες πληροφοριών-δεδομένων που καθημερινά μεταδίδονται, διαδίδονται και επεξεργάζονται είναι ανυπολόγιστες σε όγκο αλλά και σε αριθμό. Υπολογίζεται ότι 1,5 δισεκατομμύρια χρήστες, περίπου το 24% του παγκόσμιου πληθυσμού, συνδέονται με το ίντερνετ, για κάθε είδους δραστηριότητα, όπως για παράδειγμα αγορές προιόντων, παροχή υπηρεσιών on line (e-commerce,e-banking κλπ), για αναζήτηση πληροφοριών, ειδήσεων (μηχανές αναζήτησης όπως Google, Yahoo,Blogw, portals εφημερίδων), για επικοινωνία μέσω ανταλλαγής ηλεκτρονικού ταχυδρομείου (e-mail). Στις μέρες μας, γίνεται σε μεγάλο βαθμό και η χρήση εφαρμογών κοινωνικής δικτύωσης (facebook,twitter,chat rooms). Το σύνολο των δικτυακών τόπων στο ίντερνετ εκτιμάται ότι έχει ανάλθει στα 156 και πλέον εκατομμύρια. Αυτό σημαίνει ότι κάθε χρήστης έχει δυνατότητα πρόσβασης σε τεράστιες ποσότητες πληροφοριών, υπηρεσιών και άλλων αγαθών που διακινούνται μέσω διαδικτύου.

1.3 ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ ΣΤΗΝ ΕΛΛΑΔΑ

Από την Ελληνική Στατιστική Αρχή ανακοινώνονται στοιχεία για το βαθμό χρήσης των νέων τεχνολογιών από τα νοικοκυριά και τα μέλη τους. Τα στοιχεία προέρχονται από τη δειγματοληπτική Έρευνα Χρήσης Τεχνολογιών Πληροφόρησης και Επικοινωνίας από νοικοκυριά και άτομα έτους 2015.
Στην Έρευνα Χρήσης Τεχνολογιών Πληροφόρησης και Επικοινωνίας από νοικοκυριά και άτομα ερευνήθηκαν 4.667 ιδιωτικά νοικοκυριά και ισάριθμα μέλη αυτών, σε ολόκληρη την Ελλάδα, με προϋπόθεση την ύπαρξη ενός, τουλάχιστον, μέλους ηλικίας 16 – 74 ετών σε κάθε νοικοκυριό.

ΝΟΙΚΟΚΥΡΙΑ ΚΑΙ ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ–ΣΥΝΔΕΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟ ΤΗΝ ΚΑΤΟΙΚΙΑ–ΤΥΠΟΣ ΣΥΝΔΕΣΗΣ

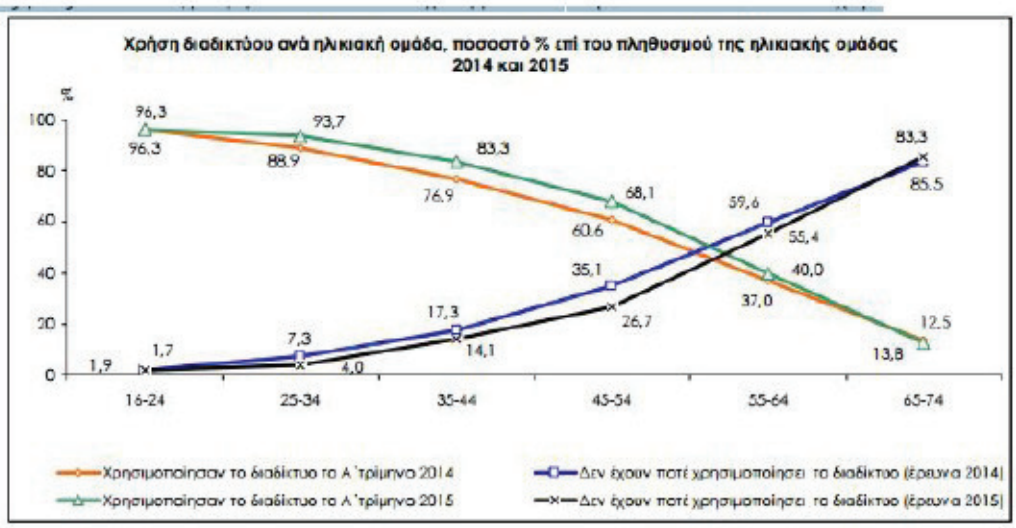
7 στα 10 νοικοκυριά έχουν πρόσβαση σε ηλεκτρονικό υπολογιστή (ποσοστό 68,6%) και πρόσβαση στο διαδίκτυο από την κατοικία τους (ποσοστό 68,1%). Την τελευταία πενταετία (2010 – 2015) καταγράφεται αύξηση 46,8% στην πρόσβαση στο διαδίκτυο από την κατοικία.

Ειδικότερα, στα ποσοστά των νοικοκυριών της Χώρας που έχουν πρόσβαση σε ηλεκτρονικό υπολογιστή και στο διαδίκτυο από την κατοικία, καταγράφεται σε σχέση με το 2014 αύξηση 7,2% και 3,8%, αντίστοιχα.
Η πρόσβαση στο διαδίκτυο ανά μεγάλη γεωγραφική περιοχή (NUTS1) παρουσιάζεται αναλυτικά στο γράφημα που ακολουθεί:

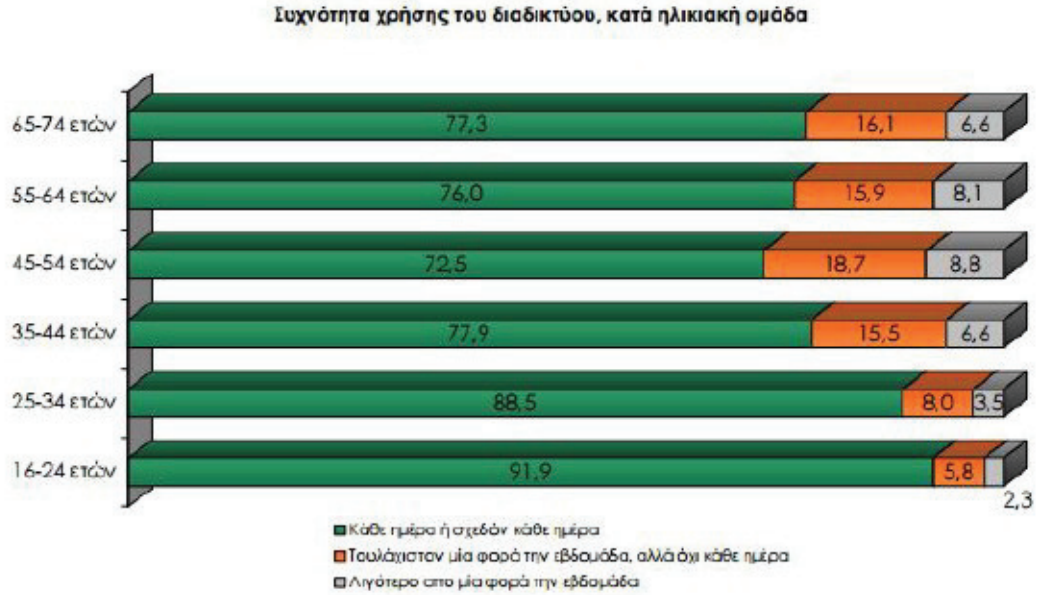
Αύξηση, σε σχέση με το 2014, καταγράφεται στην Βόρεια Ελλάδα και στην Αττική (10,4% και 5,5%, αντίστοιχα) ενώ μείωση στην Κεντρική Ελλάδα και στα Νησιά Αιγαίου και Κρήτη (3,7% και 2,6%, αντίστοιχα).
Ευρυζωνική σύνδεση χρησιμοποιεί το 67,1%, του συνόλου των νοικοκυριών της Χώρας με ένα τουλάχιστον μέλος ηλικίας 16-74 ετών, παρουσιάζοντας σε σχέση με το 2014, αύξηση 3,7%.
Διαχρονικά, η εξέλιξη των ευρυζωνικών συνδέσεων, αλλά και των συνδέσεων περιορισμένης συχνότητας από την κατοικία απεικονίζεται στο γράφημα που ακολουθεί:

Οι κυριότερο λόγοι μη πρόσβασης στο διαδίκτυο από την κατοικία είναι α) ή έλλειψη ικανοτήτων (60,7%), β) ότι οι πληροφορίες που υπάρχουν στο διαδίκτυο δεν είναι χρήσιμες, δεν ενδιαφέρουν (25,9%) και γ) ότι το κόστος του εξοπλισμού είναι πολύ υψηλό (21,7%).
Χρήση Η/Υ, κατά το Α' τρίμηνο του 2015, έκανε το 66,6% του πληθυσμού της Χώρας, ηλικίας 16 – 74 ετών.
Χρήση διαδικτύου, κατά το Α' τρίμηνο του 2015, έκανε το 66,8% του πληθυσμού της Χώρας, ηλικίας 16 – 74 ετών.
Διαχρονικά τα ποσοστά για τη χρήση Η/Υ και διαδικτύου απεικονίζονται στο γράφημα που ακολουθεί:

Κατά το Α' τρίμηνο του 2015, τόσο το ποσοστό του πληθυσμού της Χώρας που έκανε χρήση Η/Υ, όσο και αυτό που έκανε χρήση διαδικτύου παρουσίασαν αύξηση σε σχέση με το 2014. Συγκεκριμένα για τη χρήση Η/Υ και διαδικτύου καταγράφηκε αύξηση 5,2% και 5,7%, αντίστοιχα, ανάλογες με τις αυξήσεις που καταγράφηκαν το 2014 σε σχέση με το 2013 (4,8% και 5.5%, αντίστοιχα).



Για την ηλικιακή ομάδα 16-24 καταγράφεται σταθερό ποσοστό πρόσβασης στο διαδίκτυο για τα έτη 2014 και 2015. Η μεγαλύτερη αύξηση στο ποσοστό πρόσβασης (12,4%) καταγράφηκε για την ηλικιακή ομάδα 45-54 ετών. Αντίστοιχα, για όσους δεν έχουν χρησιμοποιήσει ποτέ το διαδίκτυο, η μεγαλύτερη μείωση (45,2%), σε σχέση με το 2014, καταγράφηκε για την ηλικιακή ομάδα 25-34 ετών.
Τακτική θεωρείται η χρήση του διαδικτύου, τουλάχιστον μία φορά την εβδομάδα και πραγματοποιείται από το 94,3% όσων χρησιμοποίησαν το διαδίκτυο το Α' τρίμηνο του 2015, ποσοστό αυξημένο κατά 1,0% σε σχέση με το 2014 (93,4%). Οι διαφοροποιήσεις που καταγράφονται στη συχνότητα χρήσης του διαδικτύου, κατά ηλικιακή ομάδα, παρουσιάζονται στο γράφημα που ακολουθεί:



Αναφορικά με το επίπεδο εκπαίδευσης όσων χρησιμοποίησαν το Α΄ τρίμηνο του 2015 το διαδίκτυο, το 90,3% του πληθυσμού που έχει ολοκληρώσει υψηλό επίπεδο εκπαίδευσης (μεταπτυχιακά / διδακτορικό, ΑΕΙ, ΤΕΙ, στρατιωτικές σχολές, ανώτερες σχολές τριετούς διάρκειας, κολλέγιο διάρκειας μεγαλύτερης των δύο ετών)

χρησιμοποίησε το διαδίκτυο, το 79,3% του πληθυσμού που έχει ολοκληρώσει μεσαίο επίπεδο εκπαίδευσης (δημόσιο ή ιδιωτικό ΙΕΚ, κολλέγιο διάρκειας μέχρι δύο έτη, Λύκειο (Γενικό, ΕΠΑΛ, ΤΕΛ), ΤΕΣ/ΤΕΕ (β΄ κύκλο)) και το 31,3% του πληθυσμού που έχει ολοκληρώσει χαμηλό επίπεδο εκπαίδευσης (Επαγγελματική σχολή/Τεχνική επαγγελματική σχολή/ Τεχνικό επαγγελματικό εκπαιδευτήριο (α΄κύκλο), Γυμνάσιο, Δημοτικό, δεν έχουν ολοκληρώσει ή παρακολουθήσει καμία βαθμίδα εκπαίδευσης).

ΛΟΓΟΙ ΧΡΗΣΗΣ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Η online ανάγνωση ειδήσεων σε ιστοσελίδες, εφημερίδες, περιοδικά παραμένει, όπως και το 2014, στην κορυφή της λίστας των δραστηριοτήτων που πραγματοποιούνται μέσω διαδικτύου με ποσοστό 85,4%, ενώ η αναζήτηση πληροφοριών και υπηρεσιών, είναι η δεύτερη περισσότερο πραγματοποιούμενη δραστηριότητα, με ποσοστό 80,4%.
Τα ποσοστά που καταγράφηκαν για όσους χρησιμοποίησαν το διαδίκτυο το Α΄ τρίμηνο του 2015, για δραστηριότητες που πραγματοποιούνται μέσω διαδικτύου, κατά φθίνουσα σειρά, παρουσιάζονται ακολούθως:
Διάβασμα online ειδήσεων σε ιστοσελίδες, εφημερίδες, περιοδικά 85,4%.
• Αναζήτηση πληροφοριών για προϊόντα και υπηρεσίες 80,4%.
• Αποστολή ή λήψη ηλεκτρονικών μηνυμάτων 77,1%.
• Συμμετοχή σε ιστοσελίδες κοινωνικής δικτύωσης (facebook, twitter κλπ.) 65,7%.
• Αναζήτηση πληροφοριών υγείας, σχετικά με ασθένειες, διατροφή, κακώσεις, τραύματα, παράγοντες που βελτιώνουν την υγεία κλπ. 55,7%.
Λήψη πληροφοριών μέσω ηλεκτρονικών εγκυκλοπαιδειών (wikis) με σκοπό την γνώση για οποιοδήποτε θέμα / χόμπι κλπ. 50,3%.
• Αναζήτηση πληροφοριών για θέματα εκπαίδευσης, επιμόρφωσης ή διαθεσιμότητας εκπαιδευτικών προγραμμάτων 47,7%
• Πραγματοποίηση κλήσεων ή βιντεοκλήσεων, με χρήση web κάμερας μέσω του διαδικτύου (Skype) 44,0%.
«Ανέβασμα» σε ιστοσελίδα κειμένου, φωτογραφιών, μουσικής, videos, λογισμικού κλπ. προκειμένου να τα μοιραστούμε με άλλους 34,8%.
• Χρήση υπηρεσιών για ταξίδια και καταλύματα 31,2%.
• Αναζήτηση εργασίας ή αποστολή αιτήσεων για εύρεση εργασίας 26,6%
• «Κατέβασμα» λογισμικού (εξαιρουμένου λογισμικού για παιχνίδια 22,2%
Πραγματοποίηση τραπεζικών συναλλαγών 20,8%.
• Αποστολή γνώμης για θέματα κοινωνικά ή πολιτικά σε ιστοσελίδες (π.χ. σε blogs, δίκτυα κοινωνικής δικτύωσης κλπ.) 16,3%.
• Συμμετοχή σε online διαβουλεύσεις ή ψηφοφορίες για τον καθορισμό κοινωνικών ή πολιτικών θεμάτων (π.χ. πολεοδομικό σχεδιασμό, προσυπογραφή για προώθηση αιτήματος κλπ.) 7,7%
Συμμετοχή σε ιστοσελίδες επαγγελματικής δικτύωσης (δημιουργήσατε προφίλ χρήστη, αποστείλατε μηνύματα κλπ. στο Linkedin, στο Xing κλπ.) 6,8%
• Πώληση αγαθών ή υπηρεσιών μέσω δημοπρασιών π.χ. μέσω e-Bay, 5,1%.

Συμμετοχή σε ιστοσελίδες κοινωνικής δικτύωσης (facebook, twitter κλπ.), όπως προαναφέρθηκε, καταγράφηκε για το 65,7% του πληθυσμού ηλικίας 16-74 ετών που χρησιμοποίησε το διαδίκτυο το Α' τρίμηνο του 2015, ενώ όσον αφορά στη συχνότητα πρόσβασης τακτική χρήση (τουλάχιστον μίαφορά την εβδομάδα) των μέσων κοινωνικής δικτύωσης πραγματοποιεί το 93,2% και μόλις το 6,8% λιγότερο από μια φορά την εβδομάδα.
Στο σύνολο του πληθυσμού της Χώρας ηλικίας 16-74 ετών, συμμετοχή σε ιστοσελίδες κοινωνικής δικτύωσης (facebook, twitter κλπ.), πραγματοποιεί το 43,9% και στην ηλικιακή ομάδα 16 – 24 ετών καταγράφεται το υψηλότερο ποσοστό συμμετοχής 87,5%. Αναλυτικά τα ποσοστά του πληθυσμού κάθε ηλικιακής ομάδας που συμμετείχε σε σελίδες κοινωνικής δικτύωσης εμφανίζονται στο γράφημα που ακολουθεί.

1.4 ΕΓΚΛΗΜΑ -ΗΛΕΚΤΡΟΝΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΔΙΑΔΙΚΤΥΟ

Οι Η/Υ και το ιντερνετ παρέχουν στους χρήστες ασύλληπτες δυνατότητες.Συγχρόνως όμως εισάγουν και νέες μορφές παραβατικής συμπεριφοράς. Αφενός "γεννώνται" αξιόποινες ενέργειες που είναι υπαρκτές μόνο με τη χρήση Η/Υ και του ιντερνέτ όπως η διασπορά κακόβουλου λογισμικού σε Η/Υ και η παραβίαση ηλεκτρονικών αρχείων. Από την άλλη, παραδοσιακές εγκληματικές πράξεις όπως εξύβριση ή δυσφήμιση μέσω ηλεκτρονικού ταχυδρομείου ή μιας ιστοσελίδας (web site) , διαπράττονται πλέον ευκολότερα και ταχύτερα, με το διαδίκτυο να αποτελεί το κύριο μέσο τελεσής τους. Το στοιχείο που καθιστά το διαδίκτυο πρόσφορο ως πεδίο ανάπτυξης της εγκληματικής δράσης είναι η ευχέρεια των επίδοξων δραστών να ενεργούν υπό το καθεστώς ανωνυμίας. Στις μέρες μας, παρά την εξέλιξη και ανάπτυξη των διωκτικών μηχανισμών, η διελεύκανση της ηλεκτρονικής εγκληματικότητας παραμένει μια δύσκολη υπόθεση. Συνεπώς , και εφόσον ελαχιστοποιείται κατά αυτόν τον τρόπο ο κίνδυνος τιμώρησης, ο δράστης θεωρεί πλέον τη χρήση του διαδικτύου ως ένεν εξαιρετικό προτρεπτικό παράγοντα για την τέλεση αδικημάτων.
Τι είναι όμως το ηλεκτρονικό έγκλημα; Σύμφωνα με ορισμό που δόθηκε από τους Foster και Morrison (1994) είναι "Μια εγκληματική πράξη στην οπία ο ηλεκτρονικός υπολογιστής χρησιμοποιείται ως το κυριότερο μέσο τέλεσής της". Ένας άλλος ορισμός , από τους πλέον διαδεδομένους, είναι αυτός που δόθηκε από τον Οργανισμό

Οικονομικής Συνεργασίας και ανάπτυξης , αρκετά χρόνια πριν (1986). ¨ετσι λοιπόν, “ Ηλεκτρονικό ή Ψηφιακό έγκλημα καθιστά κάθε παράνομη, ανήθικη ή χωρίς έγκριση συμπεριφορά που περιλαμβάνει την αυτόματη επεξεργασία δεδομένων ή/ και τη μετάδοση δεδομένων”

Απαραίτητο στοιχείο για την τέλεση ηλεκτρονικού εγκλήματος, θεωρείται η ύπαρξη συσκευής ηλεκτρονικής επεξεργασίας δεδομένων όπως είναι ο ηλεκτρονικός υπολογιστής, το κινητό τηλέφωνο κλπ. Σύμφωνα με τον Shinder (2002) , ο ρόλος που διαδραματίζει ο Η/Υ στα πλαίσια του ηλεκτρονικού εγκλήματος είναι κυρίαρχος καθώς:

- Μπορεί να αποτελεί το στόχο κάποιας επίθεσης, στη συγκεκριμένη περίπτωση ο Η/Υ είναι το “θύμα” της επίθεσης.
- Δύναται να αποτελεί μέσο για τη διάπραξη κάποιας επίθεσης. Εδώ είναι το εργαλείο που χρησιμοποιείται από το δράση για την πραγματοποίηση εγκληματικού σκοπού
- Τέλος , υπάρχει και η περίπτωση που ο Η/Υ αποτελεί βοηθητικό μέσο για τη διάπραξη εγκλήματος.

Μέχρι στιγμής έχουμε προσδιορίσει τον όρο “ ηλεκτρονικό έγκλημα”, τον οποίο πρέπει εν συνεχεία να διαχωρίσουμε από αυτόν του διαδικτυακού εγκλήματος.
Το διαδικτυακό έγκλημα λοιπόν ή αλλιώς κυβερνοέγκλημα (cyber-crime), είναι μια ειδικότερη μορφή του ηλεκτρονικού εγκλήματος, αυτό για του οποίου την τέλεση ο δράστης χρησιμοποιεί ειδικές γνώσεις γύρω από τον κυβερνοχώρο, κατά τον ορισμό του Donn Parker. Σχετίζεται με την οιονδήποτε μορφή κατάχρησης των δυνατοτήτων που προσφέρει το διαδίκτυο.
Αν λοιπόν θέλουμε να κατηγοριοποιήσουμε τις βασικές κατηγορίες ηλεκτρονικών εγκλημάτων, σύμφωνα με τον Αργυρόπουλο (2001), θα διακρίνουμε τα παρακάτω ηλεκτρονικά εγκλήματα:

- Εγκλήματα που διαπράττονται σε συμβατικό περιβάλλον καθώς και σε περιβάλλον ηλεκτρονικών υπολογιστών. Σε αυτήν την κατηγορία έχουμε εγκλήματα όπως η συκοφαντική δυσφήμηση που μπορεί να διαπραχθεί και σε διαδικτυακό περιβάλλον (ανάρτηση ιστοσελίδας με προσβλητικό περιεχόμενο για κάποιο πρόσωπο). Εδώ το διαδίκτυο αποτελεί απλά ένα ακόμα μέσο τέλεσης του εγκλήματος.

- Εγκλήματα που τελούνται με τη χρήση ηλεκτρονικού υπολογιστή αλλά χωρίς την ύπαρξη δικτύωσης. Τέτοιο έγκλημα θεωρείται η παράνομη αντιγραφή λογισμικού.
- Εγκλήματα που σχετίζονται αποκλειστικά με το διαδίκτυο (τα λεγόμενα διαδικτυακά εγκλήματα). Η χρήση του διαδικτύου είναι απαραίτητο στοιχείο για την εγκληματική συμπεριφορά του δράστη. Εδώ εντάσσουμε τη διασπορά κακόβουλου λογισμικού.

Μια άλλη οπτική είναι η κατηγοριοποίηση των ηλεκτρονικών εγκλημάτων που προτάθηκε από την Εξεταστική Επιτροπή της Μεγάλης Βρετανίας, ένα ανεξάρτητο σώμα που από την ίδρυση του στις αρχές της δεκαετίας του 1980, διενήργησε έρευνες με στόχο να εξακριβώσει την έκταση του εγκλήματος μέσω Η/Υ σε δημόσιο και ιδιωτικό τομέα. Οι κατηγορίες παρουσιάζονται στον παρακάτω πίνακα:

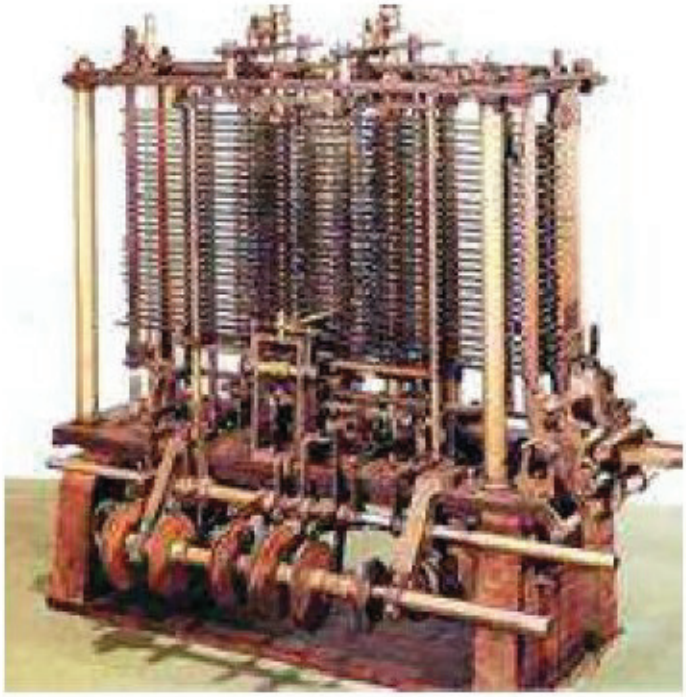
Πίνακας 1.2 : Κατηγορίες ηλεκτρονικών εγκλημάτων

ΕΓΚΛΗΜΑ-ΠΡΟΣΒΟΛΗ	ΠΕΡΙΓΡΑΦΗ
Απάτη	Για προσωπική Ωφέλεια - Αλλοίωση των εισαγομένων με νόμιμο τρόπο - Καταστροφή/συμπίεση/ακαταλληλότητα εκροών - Αλλοίωση δεδομένων του Η/Υ - Αλλοίωση ή κακή χρήση των προγραμμάτων (εξαιρουμένων των προσβολών από τους ιούς) - Των δεδομένων - Του λογισμικού - Χρήση παράνομων αντιγράφων λογισμικού - Μη εγκεκριμένη χρήση δυνατοτήτων των συστημάτων Η/Υ του οργανισμού για αποκομιδή κέρδους ή για ίδιον όφελος
Κλοπή	
Χρήση λογισμικού χωρίς άδεια	
Ιδιωτική εργασία	- Ανεπίσημη ανάγνωση των αρχείων ενός συστήματος Η/Υ και παράβαση της σχετικής νομοθεσίας - Ελεύθερη πρόσβαση σε ένα σύστημα Η/Υ συνήθως με τη χρήση των δυνατοτήτων της επικοινωνίας - Η διαμεσολάβηση με την πρόκληση ζημίας στον τρέχοντα κύκλο ή εξοπλισμό
Κακή χρήση προσωπικών δεδομένων	
Χάκινγκ Σαμποτάζ	- Εισαγωγή πορνογραφικού υλικού π.χ. Πορνογραφικού υλικού μέσω
Εισαγωγή	

	Ιντερνετ
Ιοί	Διάχυση ενός προγράμματος με σκοπό τη ματαίωση της τρέχουσας εφαρμογής

1.5 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η απαρχή του ηλεκτρονικού εγκλήματος είναι ταυτόχρονη με την εμφάνιση των ηλεκτρονικών υπολογιστών καθώς τότε έγιναν οι πρώτες προσπάθειες από επίδοξους ηλεκτρονικούς εγληματίες να βρούν τρόπους ώστε να εκμεταλλευτούν τις νέες τεχνολογίες προς όφελος τους αποκτώντας έτσι νέες ευκαιρίες για ευκολότερη και ταχύτερη διάπραξη εγκλημάτων.
Τα πρώτα χρόνια από την εμφάνιση του ηλεκτρονικού υπολογιστή,το ηλεκτρονικό έγκλημα ήταν ακόμα σπάνιο καθώς και ο αριθμός των υπολογιστών ήταν μικρός αλλά και οι γνώσεις που απαιτούνται για τον χειρισμό τους (γλώσσα μηχανής) καθιστούν τους υπολογιστές είδος πολυτελείας και συνεπώς το ηλεκτρονικό έγκλημα ήταν περιορισμένο.
Με την αλματώδη εξέλιξη των ηλεκτρονικών υπολογιστών της τελευταίας δεκαετίας του 20ου αιώνα παρατηρείται χρονικά και η ανάπτυξη του ηλεκτρονικού εγκλήματος. Στις μέρες μας , το μεγαλύτερο ποσοστό του πληθυσμού των αναπτυγμένων χωρών έχει πρόσβαση σε έναν ηλεκτρονικό υπολογιστή. Επιπλέον η χρήση του έχει απλοποιηθεί σε σε τέτοιο βαθμό, ώστε ακόμα και ένα μικρό παιδί να μπορεί να το χειρίζεται.
Ουσιαστικά, η μεγαλύτερη ανάπτυξη του ηλεκτρονικού εγκλήματος συντελείται με την εμφάνιση των δικτύων που δημιουργούν νέες διόδους πρόσβασης προς την πληροφορία. Η ζωή του σύγχρονου ανθρώπου έχει αλλάξει ριζικά καθώς με τη χρήση των δικτύων έχει ανά πάσα στιγμή πρόσβαση σε μια τεράστια δεξαμενή πληροφοριών που ολοένα και μεγαλώνει προσφέροντας ακόμα περισσότερες δυνατότητες και επιλογές στο χρήστη. Το διαδίκτυο χαρακτηρίζει την ευρεία ανάπτυξη του ηλεκτρονικού εμπορίου,την πραγματοποίηση τραπεζικών εργασιών, την άμεση επικοινωνία αλλά και την εξ αποστάσεως εκπαίδευση.
Είναι λοιπόν εύκολο να αντιληφθεί κάποιος πως με την ραγδιαία ανάπτυξη της τεχνολογίας και συγκεκριμένα των ηλεκτρονικών υπολογιστών , οι ευκαιρίες για την ανάπτυξη της ηλεκτρονικής εγκληματικότητας πολλαπλασιάζονται. Και αυτό γιατί λόγω της περιορισμένης εμπειρίας που υπάρχει σε αυτού του είδους τα εγκλήματα καθίσταται δυσκολότερη η δίωξή τους από τις αρμόδιες αρχές. Επιπλέον δεν υπάρχει ακόμα ένα σαφές νομοθετικό πλαίσιο το οποίο να μπορεί να εξετάζει το ηλεκτρονικό έγκλημα.
Το πρώτο καταγεγραμμένο Ηλεκτρονικό Έγκλημα χρονολογείται το 1820 ,όταν ο Γάλλος υφαντουργός Joseph-Marie Jacquard κατασκεύασε τον αργαλειό.



Εικόνα 1.1

Η συσκευή αυτή επέτρεπε την επανάληψη ομοίων βημάτων, κατά την ύφανση συγκεκριμένων υφασμάτων. Το γεγονός αυτό προκάλεσε ανησυχία στους υπαλλήλους του Jacquard , που φοβήθηκαν ότι απειλούνταν η παραδοσιακή τους εργασία. ¨Ετσι προκαλούσαν συχνά δολιοφθορές στο μηχάνημα, για να αποθαρρύνουν τον Jacquard να χρησιμοποιήσει τη νέα τεχνολογία.

1.6 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΓΝΩΡΙΣΜΑΤΑ ΤΩΝ ΕΓΚΛΗΜΑΤΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

1. Το διαδικτυακό έγκλημα διαπράττεται άμεσα, σε χρόνο ελάχιστων δευτερολέπτων. Η ταχύτητα τέλεσής του είναι τέτοια ώστε πολλές φορές δεν το αντιλαμβάνεται ούτε το ίδιο το θύμα. Ο δράστης επιτίθεται με τη χρήση ενός ηλεκτρονικού υπολογιστή που είναι συνδεδεμένος στο διαδίκτυο και μπορεί να εισβάλλει στα υπολογιστικά συστήματα μιας επιχείρησης ή ενός οργανισμού σε οποιοδήποτε σημείο του πλανήτη. Επομένως γίνεται εύκολα αντιληπτό, ότι δεν απαιτείται η φυσική μετακίνηση του δράστη, καθώς με το πάτημα ορισμένων πλήκτρων του υπολογιστή του να δύναται να τελέσει το έγκλημα ακόμα και από το σπίτι ή το γραφείο του.
2. Η εισβολή σε ένα υπολογιστικό σύστημα μπορεί να φαντάζει δύσκολο εγχείρημα. Στην πραγματικότητα δεν απαιτούνται ιδιαίτερες και εξειδικευμένες γνώσεις στις περισσότερες των περιπτώσεων και αυτό γιατί στο διαδίκτυο διατίθενται ελεύθερα εφαρμογές λογισμικού με τις οποίες οι επίδοξοι χάκερς μπορούν να εισβάλλουν εύκολα σε δίκτυα και υπολογιστικά συστήματα και να πραγματοποιήσουν πλήθος ηλεκτρονικών επιθέσεων.
3. Το ηλεκτρονικό έγκλημα πλήττει την πληροφορία που περιέχουν τα ηλεκτρονικά

δεδομένα. Βλάβες , φθορές καθώς και αλλοιώσεις που προκαλούνται σε ενσώματα αντικείμενα όπως σκληρούς δίσκους, μνήμες κλπ, είναι απλά δευτερεύουσες συνέπειες της κύριας προσβολής που αφορά τα δεδομένα.
4. Το ηλεκτρονικό έγκλημα εισάγει νέους νομοθετικούς περιορίσμους. Πολλές φορές είναι πολύ δύσκολο να προσδιοριστεί ο τόπος τέλεσης του εγκλήματος και αυτό γιατί με τη χρήση ενός μόνο δικτυωμένου ηλεκτρονικού υπολογιστή ο εγκληματίας μπορεί να διαπράξει από οποιοδήποτε σημείο του κόσμου. Δύσκολα προσδιορίσιμος είναι επίσης και ο ακριβής χρόνος τέλεσης του εγκλήματος και αυτό γιατί τα θύματα κατά κανόνα αντιλαμβάνονται την επίθεση και τη ζημία που προκλήθηκαν πολύ αργότερα από το χρόνο που πραγματοποιήθηκαν.
5. Με τη διερεύνηση του ηλεκτρονικού εγκλήματος συχνά απαιτείται η συνεργασία τουλάχιστον δύο κρατών (του κράτους στο οποίο γίνεται αντιληπτή η εξωτερίκευση του εγκλήματος και του κράτους όπου βρίσκονται αποθηκευμένα τα αποδεικτικά στοιχεία). Αυτός ο διασυνοριακός χαρακτήρας του ηλεκτρονικού εγκλήματος οδηγεί σε πολλές περιπτώσεις σε διαφορετική αξιολόγηση του περιεχομένου , αφού αυτό μπορεί να είναι νόμιμο στο κράτος που βρίσκεται ο δράστης ή που υπάρχουν αποθηκευμένα τα δεδομένα και να είναι παράνομο στο κράτος που τα δεδομένα λαμβάνονται ή βρίσκεται ο αποδέκτης τους.
6. Δεν υπάρχουν επαρκή στατιστικά στοιχεία τόσο στον διεθνή όσο και στον ελληνικό χώρο. Τα εγκλήματα στον κυβερνοχώρο που καταγγέλλονται είναι σχετικά λίγα και αυτό γιατί το θύμα ακόμα και όταν αντιληφθεί μια ηλεκτρονική επίθεση εναντίον του, δεν καταφεύγει στις αρμόδιες διωκτικές αρχές. Ένας από τους πιο σπουδαίους λόγους για τον δισταγμό αναφοράς του εγκλήματος , είναι ο φόβος της εταιρίας που δέχτηκε την επίθεση ότι η αποκάλυψη του γεγονότος θα επέφερε αρνητικές συνέπειες κυρίως όσο αφορά το κύρος , την αξιοπιστία και την εικόνα προς τους πελάτες.
7. Για τη διερεύνηση του ηλεκτρονικού εγκλήματος απαιτούνται εξειδικευμένες γνώσεις σε θέματα πληροφορικής τεχνολογίας και διαδικτύου καθώς και συνεχή εκπαίδευση όσων είναι ερμόδιοι για τη δίωξή του (αστυνομικές και δικαστικές αρχές).

1.7 Ο ΨΗΦΙΑΚΟΣ ΕΓΚΛΗΜΑΤΙΑΣ

Ο εντοπισμός των ψηφιακών εγκληματιών είναι τεχνολογικά περίπλοκος. Οι άνθρωποι αυτοί διαφέρουν μεταξύ τους ανάλογα με τις δεξιότητες, τους πόρους και τα κίνητρα τους. Μπορούν να έχουν διαφορετικά επίπεδα ικανοτήτων που στηρίζονται στη βασική τους εκπαίδευση , τις κοινωνικές τους αλληλεπιδράσεις και στην εμπειρία τους στη χρήση Η/Υ.
Υπάρχουν τρεις κατηγορίες ηλεκτρονικών εγκληματιών:
- Οι κατασκευαστές εργαλείων
- Οι χρήστες εργαλείων
- Οι συγραφείς προγραμμάτων

Τα κίνητρά τους περιλαμβάνουν την πλεονεξία, την ανάγκη να προβάλλουν την ευχέρειά τους στη χρήση των Η/Υ και την αδυναμία τους να κατανοήσου τη ζημιά

που προξενούν.
Σύμφωνα με τον κ. Γιάννη Πανούση, καθηγητή Εγκληματολογίας στο τμήμα Επικοινωνίας και Μ.Μ.Ε. Του Πανεπιστημίου Αθηνών:
“ Ο σύγχρονος αυτός παραβάτης του νόμου ανατρέπει εντελώς το κλασσικό στερεότυπο που απεικονίζει τον εγκληματία ως άνεργο, αμόρφωτο, φτωχό. Ο δράστης της ηλεκτρονικής εγκληματικότητας έχει τέλεια εξειδικευμένες γνώσεις και ταχνικές ικανότητες, δεν ασχολείται με την οικονομία, τη διοίκηση και τις επιχειρήσεις, διαθέτει λευκό ποινικό μητρώο και εμφορείται από κερδοσκοπικά κίνητρα ή πολιτικες φιλοδοξίες. Κανένα σύστημα ασφαλείας δεν επαρκεί όταν ο κλέφτης βρίσκεται βρίσκεται μέσα στο κύκλωμα. Απάτες σε τραπεζικά τσεκ, παράνομες παρακολουθήσεις τηλεφώνων και μαγνητοφωνήσεις συνομιλιών συνιστούν τη συνήθη πρακτική του ηλεκτρονικού εγκληματία, ο οποίος τις περισσότερες φορές εργάζεται σε υπαλληλική θέση ή σε διευθυντικό πόστο στην εταιρία ή τον οργανισμό όπου διαπράττει το έγκλημά του. Το γεγονός ότι η σωματική παρουσία του δράστη κατά την τέλεση του εγκλήματος δεν είναι απαραίτητη, καθώς και το ότι τα ηλεκτρονικά εγκλήματα δεν έχουν σύνορα, δυσχεραίνουν ακόμη περισσότερο τον εντοπισμό του δράστη , των δραστών ή του κυκλώματος”.

ΚΕΦΑΛΑΙΟ 2

Μέχρι αυτό το σημείο έχει γίνει προσπάθεια ορισμού του Ηλεκτρονικού Εγκλήματος. Έχει γίνει λόγος για τους ηλεκτρονικούς εγκληματίες και για τις απειλές του ηλεκτρονικού εγκλήματος. Στο κεφάλαιο αυτό θα γίνει διεξοδική αναφορά στις μορφές του Ηλεκτρονικού Εγκλήματος και για αυτό είναι απαραίτητος ο διαχωρισμός τους σε δυο βασικές κατηγορίες. Στην πρώτη κατηγορία έχουμε τα εγκλήματα που εμφανιστήκαν μαζί με τους ηλεκτρονικούς υπολογιστές και το διαδίκτυο και χαρακτηρίζονται ως «γνήσια» και στη δεύτερη κατηγορία εντάσσονται τα εγκλήματα που παρόλο προϋπήρχαν των ηλεκτρονικών υπολογιστών και του διαδικτύου, αυτά τα δυο συντελούν σε μεγάλο βαθμό στην εκτέλεση τους.

2.1 ΓΝΗΣΙΑ ΗΛΕΚΤΡΟΝΙΚΑ ΕΓΚΛΗΜΑΤΑ

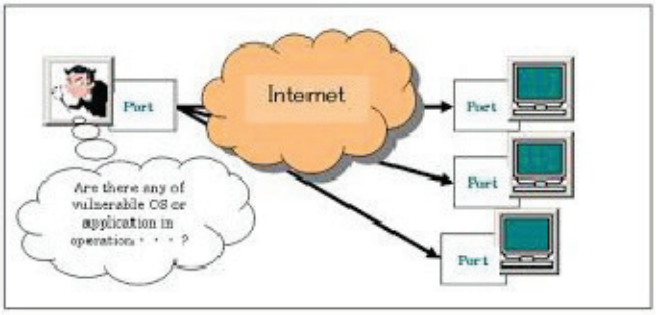
Σε αυτά συμπεριλαμβάνονται οι κακόβουλες εισβολές στα δίκτυα, (hacking). Συμπεριλαμβάνονται επίσης οι επιθέσεις άρνησης εξυπηρέτησης, το κακόβουλο λογισμικό, η ανεπιθύμητη αλληλογραφία (spamming), οι επιθέσεις σε δικτυακούς τόπους, η πειρατεία ονομάτων χώρου, το ψάρεμα (phishing) και πειρατεία λογισμικού.

2.1.1 HACKING

Το hacking είναι πλέον το έγκλημα του 21ου αιώνα και βρίσκεται σε κάθε διαδικτυακό έγκλημα. Οι hackers αποσκοπούν στην πρόσβαση ξένων υπολογιστών ή συστημάτων υπολογιστών με στόχο την διαχείριση αυτών εξ' αποστάσεως. Εισβάλλουν στο διαδίκτυο με πρόσβαση σε συστήματα, αποκτώντας γνώσεις για την ασφάλεια του και τις αδυναμίες του, κάτι το οποίο καθιστά ακόμη πιο εύκολη την επίθεση του στόχου. Ανάλογα με τα δικαιώματα που αποκτά ο εισβολέας στο σύστημα, διακρίνονται δύο κατηγορίες: α) στην πλήρη διείσδυση με δικαιώματα διαχειριστή συστήματος, όπου σε αυτή τη περίπτωση ο επιτιθέμενος μπορεί να

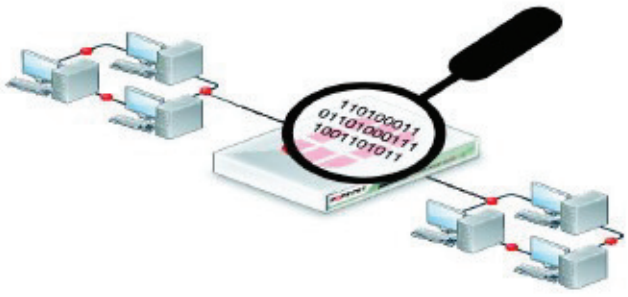
παρέμβει κάνοντας σοβαρές αλλαγές, και β) στην διείσδυση με δικαιώματα απλού χρηστή συστήματος.
Ποιες είναι όμως οι πιο συνήθεις τεχνικές hacking;
Η εκμετάλλευση των cookies:
Σε κάθε ηλεκτρονικό υπολογιστή τοποθετούνται μικρά αρχεία (cookies) από διάφορες τοποθεσίες του διαδικτύου που επισκέπτεται ο χρηστής. Σε αυτά τα αρχεία λοιπόν, ένας hacker εκμεταλλευόμενος κάποια ευπάθεια του ηλεκτρονικού συστήματος, έχει τη δυνατότητα να βρει όνομα χρηστή, κωδικούς πρόσβασης για μια υπηρεσία κ.α.

Ανίχνευση δικτυακών υπηρεσιών συστημάτων:



Στην περίπτωση αυτή οι εισβολείς προσπαθούν να συγκεντρώσουν πληροφορίες για το σύστημα – στόχο. Αυτό το πετυχαίνουν στέλνοντας ερωτήματα σε διακομιστές σχετικά με τις παρεχόμενες υπηρεσίες και το επίπεδο ασφαλείας. Αυτή είναι η τεχνική σάρωσης των θυρών (port scanning). Οι πληροφορίες που λαμβάνουν είναι σημαντικές αφού έτσι ο επιτιθέμενος μπορεί πλέον να εισβάλει στο σύστημα εκμεταλλευόμενος τις ευπάθειές του λειτουργικού συστήματος ή άλλων παρεχόμενων υπηρεσιών. Μέσω αυτών των πληροφοριών μπορεί να βρει και λογαριασμούς οι όποιοι δεν προστατεύονται με κωδικούς πρόσβασης, κάνοντας το στόχο ευκολότερο.

Ανιχνευτές δικτυακών πακέτων: Η ανίχνευση δικτυακών πακέτων πραγματοποιείται με τις εφαρμογές λογισμικού packet sniffers τα οποία παρέχουν τη δυνατότητα εντοπισμού όλων των πακέτων που υπάρχουν στο διαδίκτυο.

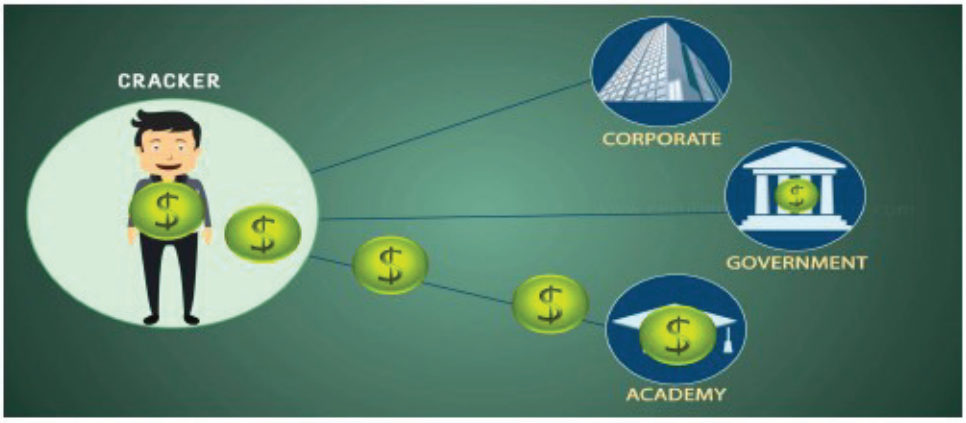


Σε περίπτωση που τα πακέτα αυτά δεν είναι κρυπτογραφημένα η απόσπαση των πληροφοριών είναι εύκολη. Ο hacker μπορεί να έχει πληροφορίες όπως είναι οι κωδικοί πρόσβασης, ο αριθμός πιστωτικών καρτών και άλλων που βρίσκονται στο διαδίκτυο.

Πλαστές διευθύνσεις: Ο ρόλος των hackers σε αυτήν τη τεχνική είναι η παρέμβαση τους σε επικεφαλίδες πακέτων μέσα σε ένα δίκτυο, τις οποίες τροποποιούν ώστε το μήνυμα να φαίνεται ότι προήλθε από αξιόπιστη πηγή. Μέσω αυτών των πλαστών διευθύνσεων εισβάλλουν αβίαστα σε δικτυακές υπηρεσίες.

Επιθέσεις σε επίπεδο εφαρμογής: Οι επιθέσεις εστιάζονται στις αδυναμίες – ευπάθειες των δικτυακών εφαρμογών. Οι φυλλομετρητές συχνά παρουσιάζουν προβλήματα στην ασφάλεια τους.

2.1.2 CRACKING



Το Cracking αποτελεί την παράνομη πρόσβαση σε ξένα υπολογιστικά συστήματα , η αλλαγή των σχετικών κωδικών πρόσβασης και η άρνηση προστασίας των προγραμμάτων που καθιστά δυνατή την παράνομη αντιγραφή τους. Βασικός σκοπός ενός Cracker είναι μέσω της μη εξουσιοδοτημένης πρόσβασης στο σύστημα υπολογιστών και των δεδομένων του, η κλοπή πληροφοριών και η πρόκληση οικονομικής ή άλλου είδους ζημιάς.Ένα πολύ γνωστό παράδειγμα κακόβουλης επίθεσης cracker είναι η υποκλοπή κωδικού πιστωτικής κάρτας τον οποίο χρησιμοποιεί προς όφελός του.

2.1.3 ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

Το κακόβουλο λογισμικό είναι ίσως ένα από τα πιο διαδεδομένα εγκλήματα στο χώρο του διαδικτύου. Η διασπορά του κακόβουλου κώδικα έχει σκοπό να διεισδύσει σε έναν ηλεκτρονικό υπολογιστή με σκοπό να του προκαλέσει ζημιά διαγράφοντας ή αλλοιώνοντας δεδομένα και προγράμματα, υποκλέπτοντας δεδομένα ή παρεμποδίζοντας τη λειτουργία ενός συστήματος.
Συμφωνά με τον Sinrod ο κακόβουλος κώδικας διακρίνεται στους ιούς, στα σκουλήκια και στους δούρειους ίππους.

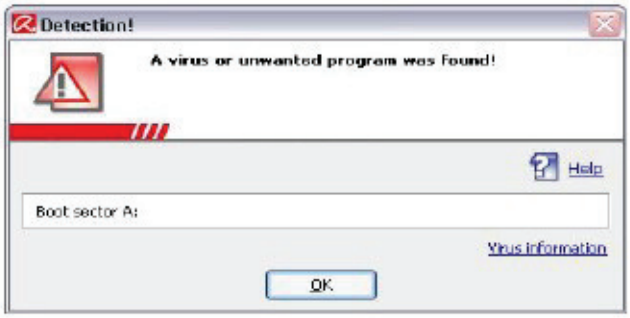
ΙΟΙ

Οι ιοί είναι ο πιο συνήθης κακόβουλος κώδικας. Ένας ιός δεν είναι τίποτα περισσότερο από ένα πρόγραμμα που τοποθετείται σε σημεία τέτοια ώστε να μην γίνεται αντιληπτός εκτελώντας την επίθεση του. Το πρόγραμμα αυτό είναι μια σειρά από εντολές που εκτελούν κακόβουλες ενέργειες σε έναν υπολογιστή. Σημαντικό είναι, όπως αναφέρθηκε και προηγουμένως, να εγκατασταθεί σε τέτοια θέση στον υπολογιστή – θύμα ώστε να μην γίνει αντιληπτό από το χρηστή. Ο χρήστης επομένως άθελα του γίνεται φορέας του ιού που θα μεταδώσει σε άλλον υπολογιστή. Έτσι επιδιώκεται η συνέχειά του ενώ παράλληλα προκαλεί ζημιές και αλλοιώσεις σε κάθε υπολογιστικό σύστημα.

Οι βασικότεροι ιοί είναι οι:

File-infectors ή parasitic viruses: ο ιός αυτός ενεργεί μολύνοντας ένα εκτελέσιμο πρόγραμμα, στο οποίο προσθέτουν το κακόβουλο κώδικα. Μολύνει αρχεία με επεκτάσεις .com, .exe, .sys, .old.

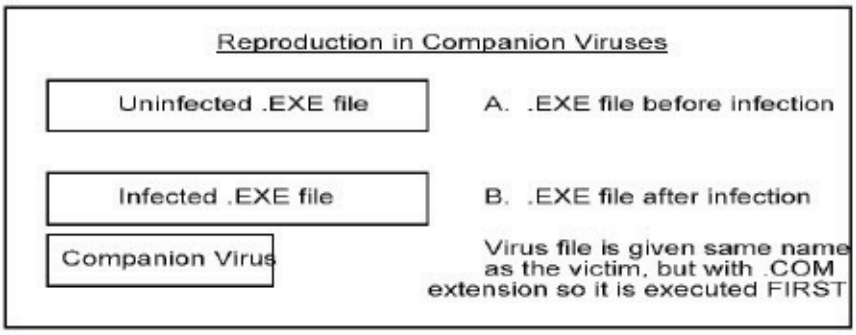
Boot Sector Virus: ο ιός αυτός προσβάλει εκτελέσιμο κώδικα συστήματος, τον οποίο εντοπίζει σε συσκευές βοηθητικής μνήμης, στον τομέα εκκίνησης ή στο MBR (Master Boot Record) του δίσκου. Ο Boot Sector Virus ενεργεί μολύνοντας κάθε δίσκο ή δισκέτα που θα χρησιμοποιηθεί από τον υπολογιστή.



Multi-partite viruses: Δρουν συνδυάζοντας επιμέρους χαρακτηριστικά των δύο παραπάνωκατηγοριών. Έχουν τη δυνατότητα να μολύνουν εκτελέσιμα αρχεία αλλά

και τομείς εκκίνησης.

Companion viruses:



Ο ιός εκμεταλλεύεται μια ευπάθεια του λειτουργικού συστήματος DOS. Μεταδίδεται με αποσπώμενα αποθηκευτικά μέσα και πολλές φόρες το αρχείο αυτό παραμένει κρυφό στη μνήμη του υπολογιστή.

Ιοί Link και Flash Bios: οι link δε μολύνουν το πρόγραμμα καθ' αυτό αλλά δρουν τροποποιώντας το αρχείο FAT (file allocation table). Αυτό έχει ως αποτέλεσμα να αλλάζει ο σύνδεσμος που δείχνει προς ένα πρόγραμμα του υπολογιστή με τρόπο ώστε να «δείχνει» στο σημείο που βρίσκεται ο ιόςκαι να εκτελείται αυτός αντί για το πρόγραμμα.
Οι Flash Bios αντικαθιστούν το λογισμικό BIOS στην μητρική πλακέτα με απρόβλεπτες συνέπειες, όπως αδυναμία εκκίνησης του υπολογιστή.

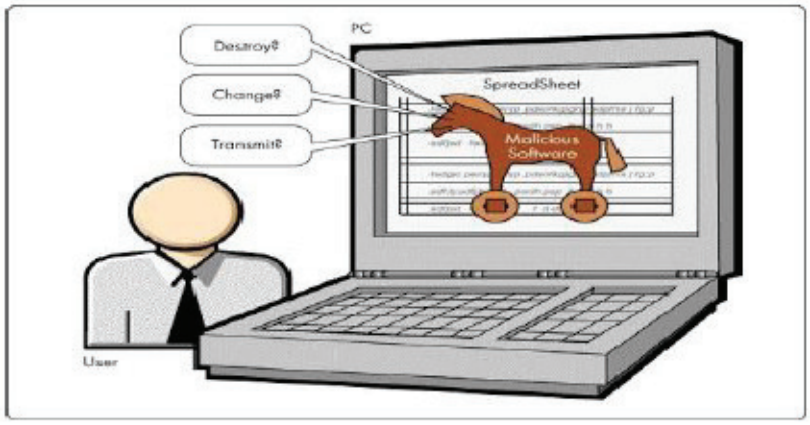
Macro viruses: οι ιοί αυτοί βρίσκονται σε αρχεία προγράμματος αυτοματισμού γραφείου.

ΣΚΟΥΛΗΚΙΑ (WORMS)

Τα σκουλήκια είναι παρόμοια με τους ιούς μόνο που πολλαπλασιάζονται χωρίς κάποια συγκεκριμένη ενέργεια από το χρήστη. Η διάδοσή τους γίνεται μέσω διαδικτύου χωρίς να χρειάζεται να επισυναφτούν σε κάποιο αρχείο. Αυτά μπορούν να τροποποιήσουν ή να διαγράψουν αρχεία ενός υπολογιστή και στη συνέχεια στέλνουν αντίγραφα του εαυτού τους σε υποψήφια θύματα. Από τα πιο καταστροφικά σκουλήκια ήταν το Code Red II που μόλυνε σε 14 ώρες 359.000 υπολογιστές προκαλώντας ζημία που ξεπερνούσε τα δύο δις. Δολάρια.

Στη κατηγορία του κακόβουλου λογισμικού περιλαμβάνονται επίσης οι Δούρειοι ίπποι, Adware, Spyware, Dialers, οι λογικές και ωρολογιακές βόμβες, οι φάρσες και οι τεχνικές απόκρυψης ιών.

ΔΟΥΡΕΙΟΙ ΙΠΠΟΙ



Στον τρωικό πόλεμο ο Οδυσσέας κατάφερε να εξαπατήσει τους Τρώες με τον Δούρειο Ίππο. Αυτό που έκανε ήταν να «δωρίσει» στους Τρώες τον Δούρειο Ίππο για να έχουν καλή τύχη. Οι Τρώες πέρασαν τον Ίππο μέσα από τα τείχη και τότε εμφανίστηκαν οι έλληνες μέσα από αυτόν ξεκινώντας την άλωση της πόλης. Έτσι λοιπόν δίνουμε αυτή την ονομασία και στο κακόβουλο λογισμικό αφού κι αυτό φαινομενικά είναι ένα «αθώο» πρόγραμμα το όποιο κρύβει λειτουργίες που δεν είναι εύκολο να εντοπιστούν από το χρήστη. Τα προγράμματα αυτά φορτώνονται στο σκληρό δίσκο του υπολογιστή. Ο επιτιθέμενος με αυτό τον τρόπο καταφέρνει τον εξ αποστάσεως έλεγχο του συστήματος και μπορεί έτσι να συλλέξει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών ή ακόμα και να εξαπολύσει άρνηση εξυπηρέτησης.

Τα Ad-ware και Spyware είναι προγράμματα που περιέχουν κακόβουλο κώδικα και θεωρούνται υποκατηγορία των Δούρειων Ίππων. Χρησιμοποιούνται για την διαφημιστική προώθηση συγκεκριμένων δικτυακών τόπων και προϊόντων που προσφέρονται μέσω του διαδικτύου. Σε περίπτωση που η λειτουργία τους ορίζεται στους όρους χρήσης που αποδέχεται ο χρήστης, δεν χαρακτηρίζεται ως κακόβουλο λογισμικό.

Τα Ad-ware και Spyware συνεργάζονται για τη δημιουργία προφίλ χρηστών με σκοπό την αποστολή στοχευόμενων διαφημίσεων αλλά μπορούν να προκαλέσουν και ανεπιθύμητα αποτελέσματα όπως είναι η καταστροφή αρχείων, οιαποσυντονισμοί του συστήματος και η επιβράδυνση της περιήγησης στο διαδίκτυο και της εν γένει λειτουργίας του υπολογιστή.
Όσο αφορά στους dialers αποτελούν υποκατηγορία των Spyware.

Είναι μικρά προγράμματα κι έχουν τη δυνατότητα να αποσυνδέουν της τηλεφωνική γραμμή από το internet και να συνδέονται με άλλες κλήσεις μεγαλύτερης χρέωσης. Επομένως το αποτέλεσμα αυτής της λειτουργίας είναι ο πλουτισμός συγκεκριμένων κατόχων δικτυακών τόπων από τα τεράστια αυτά ποσά. Οι dialers κρύβονται σε συγκεκριμένες ιστοσελίδες οι οποίες πιθανόν περιέχουν πειρατικό λογισμικό ή οποιοδήποτε άλλο αμφιλεγόμενο λογισμικό.

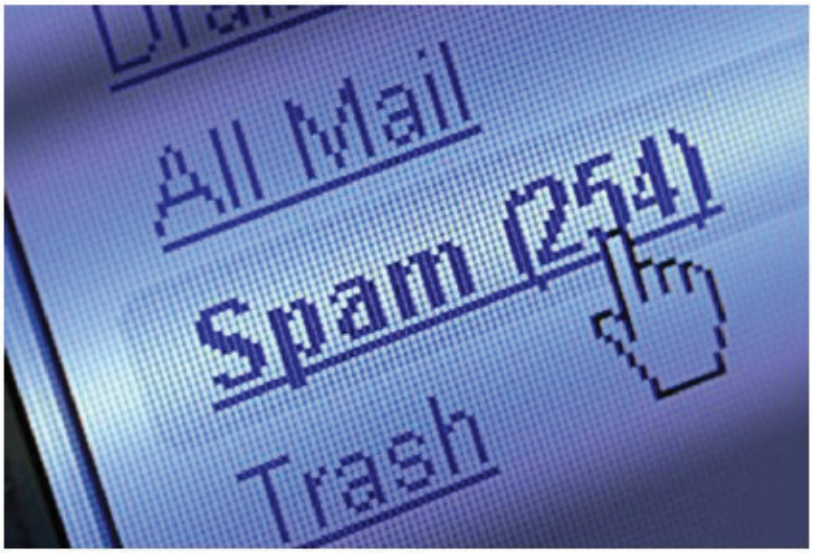
ΑΛΛΑ ΕΙΔΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Η λογική βόμβα είναι ένα πρόγραμμα που ενεργοποιείται με ένα συγκεκριμένο γεγονός. Το πρόγραμμα αυτό μπορεί να σταματήσει τη λειτουργία του υπολογιστή και να απελευθερώσει ένανιό διαγράφοντας αρχεία και προκαλώντας γενικότερες ζημιές. Το εν λόγω πρόγραμμα ενεργοποιείται είτε από το χρήστη, είτε σε χρόνο και ημερομηνία που έχει εκ των προτέρων προγραμματισθεί, όπως συμβαίνει και με τις ωρολογιακές βόμβες.

Οι φάρσες ίσως να μην ανήκουν στο κακόβουλο λογισμικό αλλά είναι κακόβουλη η πρόθεση του επιτιθέμενου, αφού το μόνο που καταφέρνει είναι να προκαλέσει πανικό στο χρήστη προειδοποιώντας τον για έναν ιό που δεν υπάρχει. Ο χρηστής ωστόσο στην προσπάθεια του να προστατέψει τα δεδομένα του καταφεύγει στη διαγραφή αυτών.
Για την προστασία του χρήστη από τους ιούς εταιρείες αντιβιοτικού λογισμικού προσφέρουν το αντίστοιχο λογισμικό για την αντιμετώπιση τους. Ωστόσο, οι αόρατοι ιοί (stealth) προβλέποντας αυτές τις κινήσεις, παραμένουν ενεργοί, κάνοντας τις καταστροφικές λειτουργίες τους χωρίς να μπορούν να εντοπιστούν από το εκάστοτε αντιβιοτικό λογισμικό.
Οι πολυμορφικοί ιοί (Polymorphic, self-mutating) παράγουν αντίγραφα του εαυτού τους,διαφορετικά μεταξύ τους αλλά το ίδιο καταστροφικά. Τα αντίγραφα δημιουργούν ένα «θόρυβο» με αποτέλεσμα να μην εντοπίζονται από τα antivirus.

2.1.4 ΑΝΕΠΙΘΥΜΗΤΗ ΑΛΛΗΛΟΓΡΑΦΙΑ (SPAMMING)

Με τον όρο spam χαρακτηρίζουμε τη μαζική αποστολή μηνυμάτων, συνήθως διαφημιστικών, που περιλαμβάνουν πληροφορίες για την προώθηση προϊόντων ή υπηρεσιών.



Η εύρεση των διευθύνσεων είναι μια σχετικά εύκολη διαδικασία αφού οι spammers παίρνουν τις διευθύνσεις από καταλόγους εταιρειών που διατηρούν ηλεκτρονικά καταστήματα ή χρησιμοποιούν λογισμικό τύπου harvester, που σαρώνει όλο το διαδίκτυο και συλλέγει διευθύνσεις από καταλόγους, από δωμάτια συζητήσεων κλπ. Επομένως μια τέτοια εφαρμογή είναι επόμενο να έχει και την αρνητική της λειτουργία εννοώντας πως είναι μια άριστη ευκαιρία για επιθέσεις.

2.1.5 ΠΕΙΡΑΤΕΙΑ ΟΝΟΜΑΤΩΝ ΧΩΡΟΥ

Η συγκεκριμένη «γνήσια» επίθεση ήταν έντονη κυρίως στα πρώτα χρόνια του

διαδικτύου, όπου οι εταιρείες δεν είχαν ακόμη κατοχυρώσει διεύθυνση στο διαδίκτυο, κάτι το όποιο πρόλαβαν να πράξουν επιτήδειοι. Έτσι είτε πωλούσαν, έναντι μεγάλου χρηματικού πόσου, τη διεύθυνση στην ενδιαφερόμενη εταιρεία, είτε χρησιμοποιώντας το κύρος του ονόματος της εταιρείας προέβαιναν σε αναρτήσεις προσβλητικού περιεχομένου.

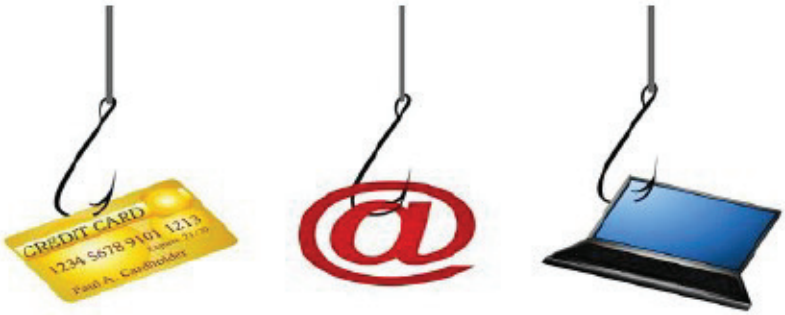
Βασική προϋπόθεση για την άσκηση ηλεκτρονικού εμπορίου αποτελεί η δημιουργία ενός χώρου στο διαδίκτυο, όπου θα καθίσταται δυνατή η πρόσβαση πελατών και η κατάρτιση των συναλλαγών. Μέσο (εισιτήριο) για την είσοδο στο διαδίκτυο αποτελεί το «domain name» (όνομα πεδίου ή όνομα χώρου), το οποίο κατ' ουσίαν επιτελεί ρόλο ηλεκτρονικής διευθύνσεως ή «κυβερνοδιευθύνσεως», επιτρέποντας την επικοινωνία του χρήστη του διαδικτύου με τον κάτοχο της ηλεκτρονικής διευθύνσεως. Το «domain name» αποτελείται από σειρά αλφαριθμητικών χαρακτήρων (τουλάχιστον τριών και όχι περισσότερων των είκοσι τεσσάρων), χωρίς ή με λογικό ειρμό, σε μια ή περισσότερες λέξεις που χωρίζονται από διάφορα σημεία, διαιρείται δε σε τρία μέρη. Το πρώτο μέρος είναι κοινό για όλα τα «domain names» και αποτελείται από τα αρκτικόλεξα «http://www» (Hyper Text Transfer Protocol – World Wide Web) που δηλώνει το πρωτόκολλο επικοινωνίας και ότι η επικοινωνία διεξάγεται στο World Wide Web (παγκόσμιο διαδίκτυο). Το δεύτερο μέρος (second level domain – SLD) ή Μεταβλητό Πεδίο αποτελείται από τα εκάστοτε ονόματα φυσικών και νομικών προσώπων, ολόκληρα ή σε συντομογραφία. Πρόκειται για το κατ' εξοχήν όνομα, την κατ' εξοχήν διαδικτυακή διεύθυνση. Το τρίτο μέρος αποτελεί το επονομαζόμενο top level domain (TLD), που δηλώνει το είδος της τοποθεσίας (ιστοθέσης) ή τη γεωγραφική προέλευση, όπως «.com» για όσους ασκούν εμπορική δραστηριότητα, «.edu» για εκπαιδευτικούς οργανισμούς, «.org» για οργανισμούς, «.net» για παροχές υπηρεσιών διαδικτύου, «.gov» για κυβερνητικούς οργανισμούς, «.int» για διεθνείς οργανισμούς, «.gr» για τη χώρα αρχειακής καταχωρίσεως του «domain name» του χρήστη, εν προκειμένω για την Ελλάδα Το «domain name» δεν μπορεί κατ' αρχήν να ταυτιστεί με την εμπορική επωνυμία, τον διακριτικό τίτλο και το εμπορικό σήμα. Πρέπει, ωστόσο, να αποδίδεται σ' αυτό λειτουργία τόσο διακριτικού τίτλου όσο και σήματος, κατά έμμεσο τρόπο, όταν αυτό χρησιμοποιείται ως διακριτικό στοιχείο για το πρόσωπο ή την επιχείρηση στο διαδίκτυο, διότι, έχει πρωταρχικά εξατομικευμένη και αναγνωριστική λειτουργία. Η ευχέρεια ελεύθερης χρήσεως οποιασδήποτε ονομασίας, όσο γνωστή και φημισμένη και αν είναι, από τον πρώτο τυχόντα, θα προκαλούσε τεράστιες ή ανεπανόρθωτες ζημίες στην επιχείρηση

που καθιερώθηκε στις συναλλαγές με την επίμαχη ονομασία. Για τη διαφύλαξη έτσι των νομίμων συμφερόντων των παραπάνω επιχειρήσεων, θα πρέπει να αποδοθεί στο «domain name» μια οιονεί λειτουργία διακριτικού τίτλου και σήματος. Τούτο ενισχύεται και από το ότι οι κάτοχοι «domain names» στην πράξη εμφανίζονται στο διαδίκτυο με τα διακριτικά γνωρίσματα που τους κατέστησαν γνωστούς στον υλικό κόσμο, δηλαδή χρησιμοποιούν το όνομα, την επωνυμία ή το σήμα τους, δεδομένων μάλιστα των περιορισμένων ορίων παροχής «domain names» για κάθε χρήση αλλά και της επιβαλλόμενης συντομίας γι' αυτού του είδους την επικοινωνία.

2.1.6 ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ

Το ηλεκτρονικό "ψάρεμα" είναι ένας τρόπος εξαπάτησης των χρηστών υπολογιστών με στόχο να τους κάνει να αποκαλύψουν προσωπικές πληροφορίες ή οικονομικά στοιχεία, μέσω ενός παραπλανητικού μηνύματος ηλεκτρονικού ταχυδρομείου ή μιας παραπλανητικής τοποθεσίας Web. Μια συνηθισμένη απάτη ηλεκτρονικού "ψαρέματος" ξεκινά με ένα μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο μοιάζει με μια επίσημη ειδοποίηση από αξιόπιστη πηγή, όπως τράπεζα, εταιρεία πιστωτικής κάρτας ή ευυπόληπτη εταιρεία ηλεκτρονικού εμπορίου. Οι παραλήπτες του μηνύματος ηλεκτρονικού ταχυδρομείου κατευθύνονται στο να επισκεφθούν μια τοποθεσία Web , η οποία έχει δημιουργηθεί με στόχο την εξαπάτησή τους, όπου τους ζητείται να παράσχουν προσωπικές πληροφορίες, όπως ο αριθμός ή ο κωδικός πρόσβασης κάποιου λογαριασμού τους. Στη συνέχεια, οι πληροφορίες αυτές χρησιμοποιούνται συνήθως για την υποκλοπή ταυτότητας.

2.1.6.1 PHISHING



"Το Phishing είναι μια νέα μέθοδος εξαπάτησης των καταναλωτών ενός οργανισμού, συνήθως κερδοσκοπικού, και συνίσταται κυρίως στην απατηλή υφαρπαγή των εμπιστευτικών πληροφοριών των καταναλωτών, όπως προσωπικά ή ευαίσθητα δεδομένα, οικονομικά δεδομένα κλπ, με σκοπό την παράνομη χρήση τους από τον Phisher για την πρόκληση βλάβης ξένης περιουσίας. Με τη βοήθεια κυρίως της απρόσκλητης εμπορικής επικοινωνίας—το γνωστό Spam—ή χρησιμοποιώντας bots για την αυτοματοποιημένη στόχευση των υποψήφιων θυμάτων τους ή άλλες παρόμοιες μεθόδους, οι Phishers, εμφανιζόμενοι κυρίως στο διαδίκτυο ως εκπρόσωποι ενός οργανισμού τα χαρακτηριστικά του οποίου έχουν αντιγράψει

παράνομα, προβαίνουν σε δόλιες πράξεις ή παραλείψεις με τις οποίες πείθουν τα στοχευμένα θύματά τους, τα οποίαενδέχεται να είναι άδηλα, ν' αποκαλύψουν ή ισάγουν σε σύστημα ηλεκτρονικών υπολογιστών στοιχεία της ταυτότητάς τους και εμπιστευτικές πληροφορίες με σκοπό να χρησιμοποιήσουν οι Phishers αυτές τις πληροφορίες για να προσπορίσουν στον εαυτό τους ή τρίτον παράνομο περιουσιακό όφελος προξενώντας βλάβη σε περιουσιακά στοιχεία των θυμάτων τους." (Παπαδόπουλος, 2005)
Αυτός ο τρόπος δράσης των εγκληματιών έχει παρατηρηθεί τα τελευταία χρόνια κι έχει σαν σκοπό την απόσπαση πληροφοριών των θυμάτων, με σκοπό την εκμετάλλευσή τους, όπως είναι οι κωδικοί του συστήματος, ο αριθμός πιστωτικών καρτών, κωδικοί πρόσβασης. Ο τρόπος δράσης είναι η εξαπάτηση του θύματος με παραπλανητικά e-mail. Για παράδειγμα, το θύμα θα δεχθεί ένα e-mail από μια ίσως τραπεζική υπηρεσία που θα του ζητήσει την επιβεβαίωση κωδικών στα πλαίσια μιας συντήρησης ή ανασυγκρότησης του συστήματος. Με αυτό τον τρόπο το ίδιο το ανυποψίαστο θύμα επιβεβαιώνει τα προσωπικά στοιχειά και τους κωδικούς στους επιτήδειους.

"Η ονομασία Phishing αναφέρεται χρησιμοποιούμενη για πρώτη φορά το 1996 από χάκερς που έκλεβαν ή παράνομα ιδιοποιούνταν τους λογαριασμούς νομίμων χρηστών της εταιρίας America Online (AOL) με παράνομη χρήση κωδικών πρόσβασης που ανήκαν σε ανυποψίαστους χρήστες—συνδρομητές της AOL. Η πρώτη αναφορά στο Διαδίκτυο για το Phishing έγινε σε newsgroup χάκερς γνωστό ως alt.2600 τον Ιανουάριο του 1996, και η πρώτη αναφορά των μέσωνενημέρωσης στο Phishing χρονολογείται τον Μάρτιο του 1997.
Οι επιθέσεις Phishing συνίστανται σ' ένα μείγμα δόλιας χρήσης τεχνολογικών μέσων αποβλέποντας στην εξαπάτηση των καταναλωτών (technical deceit) και εφαρμοσμένων μηχανιστικών πρακτικών εξαπάτησης (social engineering practices).
Σε όλες τις περιπτώσεις επιθέσεων Phishing, ο Phisher υποδύεται τον εκπρόσωπο έμπιστης πηγής πληροφοριών που,δήθεν, σχετίζεται με το θύμα, προκειμένου να πείσει το θύμα να του αποκαλύψει εμπιστευτικές πληροφορίες ή να προβεί σε πράξεις αποκάλυψης της ταυτότητας του θύματος.
Συνήθως ο Phisher επικοινωνεί με το υποψήφιο θύμα του και ισχυρίζεται ότι εργάζεται σε τράπεζα ή άλλη εταιρία που μπορεί να σχετίζεται με τον λήπτη της επικοινωνίας δίνοντάς του όλες τις απαραίτητες λεπτομέρειες για την πιστοποίησή του—ονοματεπώνυμο, αριθμός εργαζομένου, τηλέφωνο για επιβεβαίωση των στοιχείων του κλπ. Εν συνεχεία, ο Phisher ενημερώνει τον λήπτη της επικοινωνίας

του ότι, δήθεν, η πιστωτική του κάρτα ή ο τραπεζικός λογαριασμός του έχουν καταχωρηθεί σε λίστα παρακολούθησης για ασυνήθιστη συναλλακτική συμπεριφορά. Κατά την επικοινωνία του, ο Phisher επιχειρεί ν' αλιεύσει, ρωτώντας το θύμα του, κάθε πληροφορία που θα μπορούσε εν συνεχεία να χρησιμοποιήσει για να απαλείψει κάθε αμφιβολία του θύματος για τηνταυτότητα του προσώπου με το οποίο επικοινωνεί. Αφού επιτύχει την πλάνη του θύματος αναφορικά με την ταυτότητα του Phisher με παράσταση ψευδών γεγονότων ως αληθινών ή αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων, ο Phisher οδηγεί το θύμα σε πράξεις περιουσιακής διάθεσης, από τις οποίες άμεσα ή έμμεσα αποκομίζει περιουσιακό όφελος ο Phisher επί ζημία του διαθέτοντος. Η επικοινωνία στις επιθέσεις Phishing μπορεί να διεξαχθεί με ηλεκτρονικό ταχυδρομείο, με χρήση πλαστών διαδικτυακών τόπων, με εργαλεία στιγμιαίας επικοινωνίας, με τηλεφωνική επικοινωνία, και με χρήση παραβιασμένων ως προς την ασφάλειά τους διακομιστές—servers.

Οι περισσότερες επιθέσεις Phishing συνήθως γίνονται με χρήση ηλεκτρονικού ταχυδρομείου. Οι συνηθέστερες μέθοδοι που χρησιμοποιούνται για επιθέσεις Phishing με ηλεκτρονικό ταχυδρομείο περιλαμβάνουν:

1. χρήση ηλεκτρονικής αλληλογραφίας που μοιάζει να έχει σταλεί από έμπιστη πηγή
2. χρήση αντίγραφων ηλεκτρονικής αλληλογραφίας στα οποία έχουν γίνει αλλαγές σε περιεχόμενα URLs και hyperlinks
3. χρήση HTML ηλεκτρονικής αλληλογραφίας στην οποία έχουν γίνει αλλαγές σε περιεχόμενα URLs και hyperlinks
4. χρήση ιών (viruses) και σκουληκιών (worms) συνημμένων σε ηλεκτρονική αλληλογραφία
5. χρήση αντι-spam εργαλείων
6. χρήση εξατομικευμένης ηλεκτρονικής αλληλογραφίας
7. χρήση ηλεκτρονικής αλληλογραφίας με τροποποιημένη ένδειξη αποστολέα—'Mail From:' σε συνδυασμό με χρήση Open Mail Relays διακομιστών για την απόκρυψη της προέλευσης της ηλεκτρονικής αλληλογραφίας.

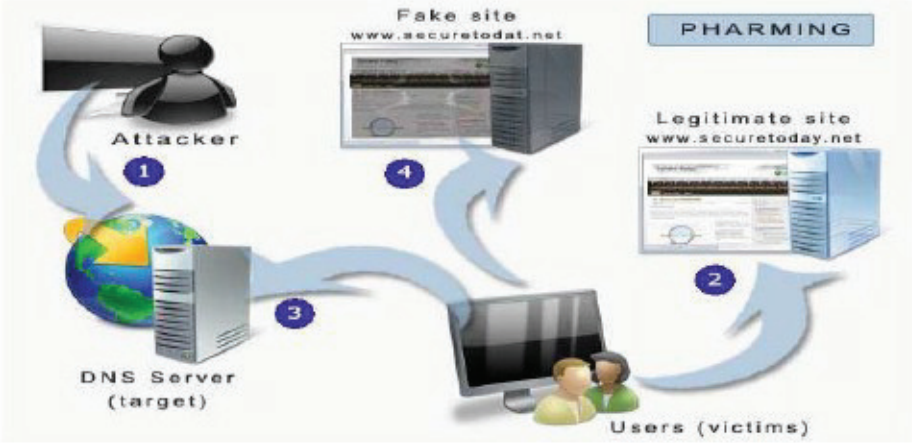
Οι συνηθέστερες μέθοδοι που χρησιμοποιούνται για επιθέσεις Phishing με χρήση

πλαστών διαδικτυακών τόπων περιλαμβάνουν:
1. εισαγωγή παραπλανητικών hyperlinks σε δημοφιλείς διαδικτυακούς τόπους
2. χρήση παραπλανητικών γραφικών ή διαφημιστικών πινακίδων (banners κλπ) με σκοπό να δελεάσουν του επισκέπτες του διαδικτυακού τόπου που τα περιέχει για να κάνουν click σ' αυτά
3. χρήση διαδικτυακών bugs ικανών να ιχνηλατήσουν την επισκεψιμότητα και συμπεριφορά των
καταναλωτών στο διαδικτυακό τόπο που τα περιέχει
4. χρήση pop-ups ή frameless windows για τη μεταμφίεση της αληθινής προέλευσης του ηλεκτρονικού μηνύματος του Phisher
5. ενσωμάτωση κακόβουλου λογισμικού κώδικα μέσα σε ιστοσελίδα ή διαδικτυακό τόπο που εκμεταλλεύεται μια γνωστή αδυναμία ασφαλείας των browsers των καταναλωτών και εγκαθιστά στο υπολογιστικό σύστημα των καταναλωτών λογισμικό της επιλογής του Phisher (π.χ. Keyloggers, Screen-grabbers, Back-doors, Trojan Horses, Wabbits, Viruses, Worms, Spyware, Exploits, Rootkits, Dialers, κλπ).
6. κατάχρηση προδιαγραφών σχέσεων εμπιστοσύνης δημιουργημένων στα πλαίσια λογισμικώνbrowsing—φυλλομετρητών ιστοσελίδων στο Διαδίκτυο—με σκοπό τη διείσδυση στα υπολογιστικά συστήματα των καταναλωτών και την τοποθέτηση εγκεκριμένων εκτελέσιμων λογισμικών προγραμμάτων—site-authorized scriptable components—στις περιοχές αποθήκευσης δεδομένων των υπολογιστικών συστημάτων των καταναλωτών".

2.1.6.2 Pharming

Το pharming είναι μια πρόσφατη μορφή εγκλήματος που έχει και αυτή σαν στόχο την κλοπή προσωπικών δεδομένων των χρηστών. Αλλά έχει διαφορές στο πως επιτυγχάνεται σε σχέση με το phising.Ένας hacker είναι αυτός που με κάποιους τρόπους καταφέρνει να ανακατευθύνει τους επισκέπτες ενός site σε ένα άλλο «ψεύτικο».Το pharming μπορεί να επιτευχθεί αλλάζοντας το hosts file στον υπολογιστή του θύματος.Το αρχείο αυτό είναι εγκατεστημένο στο σύστημα του Η/Υ και είναι υπεύθυνο για να συγκεντρώνει τις IP διευθύνσεις του χρήστη.

Ένας ακόμη τρόπος επίθεσης είναι η εκμετάλλευση των τρωτών σημείων του λογισμικού ενός DNSserver. Ένας τέτοιος server είναι υπεύθυνος στο να «μεταφράζει» τα ονόματα των διευθύνσεων τουInternet σε IP addresses. Υπάρχουν όμως σημεία στο λογισμικό αυτών των servers που μπορούν να χαρακτηριστούν τρύπες ασφαλείας που συνήθως είναι εκμεταλλεύσιμες από τους hackers.



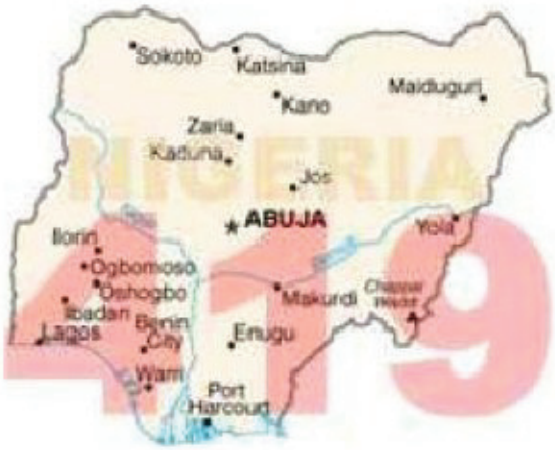
Ο τρόπος δράσης με την ονομασία «Pharming» ξεκινά από τη μη εξουσιοδοτημένη πρόσβαση και εν συνεχεία διαχείριση του DNS (Domain System Name) ιστοσελίδων οικονομικού κυρίως ενδιαφέροντος, όπως είναι για παράδειγμα οι ιστοσελίδες των τραπεζών και των ηλεκτρονικών καταστημάτων. Προκειμένου να αντιληφθούμε όμως πώς λειτουργεί το «Pharming» ως τεχνική, θα πρέπει να ρίξουμε μια ματιά στη λειτουργία του DNS. Το σύστημα που ονομάζεται DNS λειτουργεί ως ένας «ηλεκτρονικός μεταφραστής» αφού στην ουσία «μεταφράζει το όνομα της ιστοσελίδας που εμείς πληκτρολογούμε, στην αντίστοιχη IP διεύθυνση που της αναλογεί». Είναι γνωστό ότι το διαδίκτυο δεν λειτουργεί με ονομασίες ιστοσελίδων, αλλά με IP διευθύνσεις. Προκειμένου λοιπόν να συνδεθεί κάποιος χρήστης με κάποια ιστοσελίδα, η IP διεύθυνση που έχει ο χρήστης εκείνη τη στιγμή συνδέεται με την αντίστοιχη IP διεύθυνση της ιστοσελίδας. Σε όλες τις ιστοσελίδες που υπάρχουν στο internet αντιστοιχεί μία IP διεύθυνση. Ο άνθρωπος όμως είναι πολύ πιο εύκολο να θυμάται ονόματα παρά αριθμούς. Είναι πιο εύκολο να θυμάται την ιστοσελίδα www.securitymanager.gr, για παράδειγμα, παρά την IP διεύθυνση που αντιστοιχεί σε αυτήν. Όταν εμείς λοιπόν πληκτρολογούμε την αγαπημένη μας ιστοσελίδα στο διαδίκτυο, το διαδίκτυο δεν την «καταλαβαίνει» από το όνομά της και μας συνδέει με αυτή. Μέσω ειδικών διακομιστών που ονομάζονται «DNS Servers» μεταφράζει το όνομα που εμείς πληκτρολογήσαμε στην IP διεύθυνση στην οποία αντιστοιχεί και μας συνδέει με αυτήν. Η διεργασία λοιπόν μετατροπής του ονόματος που πληκτρολογούμε εμείς σε IP διεύθυνση και η σύνδεσή μας εν συνεχεία με αυτήν, πραγματοποιείται μέσω του DNS. Όπως αναφέραμε και παραπάνω, η τεχνολογία του DNS αναπτύχθηκε για εξυπηρέτηση των αναγκών των χρηστών, καθόσον είναι πολύ πιο εύκολο να θυμούνται ονόματα παρά αριθμούς.
Το «Pharming» επεμβαίνει σε αυτήν ακριβώς τη διαδικασία του DNS. Όταν ο ανυποψίαστος χρήστης πληκτρολογεί την ονομασία της ιστοσελίδας της τράπεζάς του - για παράδειγμα - και επιχειρεί να συνδεθεί με αυτήν, οι «Pharmers», χρησιμοποιώντας ειδικές τεχνικές «δηλητηριάζουν» τους DNS διακομιστές (servers) και εν συνεχεία καταφέρνουν και «ανακατευθύνουν» το χρήστη όχι στη γνήσια ιστοσελίδα της τράπεζας, αλλά σε άλλη «πλαστή» ιστοσελίδα, την οποία διαχειρίζονται εκείνοι. Συνεπώς, όταν ο χρήστης πληκτρολογεί τους κωδικούς

web-banking για να μπει στο λογαριασμό του, «δίνει» ουσιαστικά τους κωδικούς αυτούς στους «Pharmers», αφού τους πληκτρολογεί σε ιστοσελίδα που διαχειρίζονται εκείνοι. Στη συνέχεια, εκείνοι τους εκμεταλλεύονται αναλόγως.
Το «Pharming», εκτός από τον τρόπο που προαναφέρθηκε μπορεί να γίνει και μέσα από τη μη εξουσιοδοτημένη πρόσβαση και τροποποίηση του λεγόμενου «host file» του ηλεκτρονικού υπολογιστή του χρήστη. Ο συγκεκριμένος φάκελος με την επωνυμία «host file» χρησιμοποιείται από το λειτουργικό σύστημα του ηλεκτρονικού υπολογιστή (π.χ. windows), προκειμένου να αντιστοιχίσει τα «hostnames » με IP διευθύνσεις. Και εδώ οι «Pharmers» μπορούν να επέμβουν, να αλλάξουν την αντιστοιχία αυτή και ο χρήστης να οδηγηθεί σε μη γνήσια ιστοσελίδα που ελέγχεται από αυτούς.
Όπως έχει ήδη αναφερθεί, το «Pharming» στοχοποιεί ιστοσελίδες οικονομικού κυρίως ενδιαφέροντος, αφού από εκεί οι «Pharmers» μπορούν να αντλήσουν κέρδη. Θα αναφέρουμε στο σημείο αυτό ότι η συγκεκριμένη τεχνική χρησιμοποιείται για ελάχιστο χρονικό διάστημα, καθόσον μπορεί να γίνει εύκολα αντιληπτή από τους διαχειριστές των ιστοσελίδων που δέχονται την επίθεση. Με άλλα λόγια, οι «Pharmers» εφαρμόζουν την τεχνική τους για μικρό χρονικό διάστημα, προκειμένου να υποκλέψουν τους κωδικούς συγκεκριμένου αριθμού χρηστών και εν συνεχεία επαναφέρουν το σύστημα στην κανονική του κατάσταση. Σημαντικό σε αυτήν την τεχνική είναι το γεγονός ότι οι τραπεζικοί και πιστωτικοί Οργανισμοί (οι οποίοι δέχονται και το μεγαλύτερο αριθμό τέτοιων επιθέσεων), δεν αναφέρουν τις επιθέσεις που δέχονται. Προτιμούν να τις διαχειρίζονται εσωτερικά, καθόσον η δημοσιοποίηση τέτοιων επιθέσεων, φυσικά, θα προκαλέσει ζημία στο κύρος, τη φήμη και την αξιοπιστία τους.

2.1.7 ΑΠΑΤΗ ΜΕ ΤΗ ΝΙΓΗΡΙΑΝΗ ΕΠΙΣΤΟΛΗ

Η Νιγηριακή απάτη είναι μηνύματα ηλεκτρονικού ταχυδρομείου (e-mail) που περιέχουν πλασματικές ιστορίες μέσω των οποίων οι δράστες προσπαθούν να αποσπάσουν μεγάλα χρηματικά ποσά από ανυποψίαστους χρήστες, δελεαζοντάς τους με τεράστια κέρδη. Ο αποστολέας- απατεώνας συστήνεται ως ένα σημαντικό πρόσωπο του καθεστώτος την Νιγηρίας (συνήθως ως κάποιος υψηλόβαθμος αξιωματούχος ή στέλεχος κρατικής εταιρίας). Επικαλούμενος κυρίως λόγους πολιτικής φύσεως , ο δράστης ζητάει τη βοήθεια του θύματος- παραλήπτη της επιστολής, προκειμένου να διοχετεύσει εκτός χώρας (Νιγηρίας) κάποιο τεράστιο χρηματικό ποσό. Με άλλα λόγια το ανυποψίαστο θύμα καλείται να διεκολύνει το δράστη λειτουργώντας ως αποδέκτης του ποσού έτσι ώστε να γίνει δεκτή από την κυβέρνηση η διοχέτευση των χρημάτων εκτός Νιγηρίας. Για τη βοήθεια που θα προσφέρει θα ανταμειφθεί με προμήθεια ένα σημαντικό χρηματικό ποσό. Όταν το σύνολο του ποσού θα έχει μεταφερθεί στον τραπεζικό του υποψήφιου θύματος τότε υποτίθεται ότι έναντι μιας υψηλής προμήθειας θα πρέπει να το παραδώσει στον αποστολέα του e-mail. Αρχικά αυτό που ζητείται είναι η συγκατάθεση του παραλήπτη του e-mail και η παροχή πληροφοριών σχετικά με τους τραπεζικούς του

λογαριασμούς και άλλων στοιχείων που θα βοηθούσαν στην πραγματοποίηση της συναλλαγής. Η επόμενη φάση της απάτης ξεκινάει από τη στιγμή που κάποιος αποφασίζει να απαντήσει στην αρχική προσφορά και έτσι να την αποδεχθεί. Ξεκινάει λοιπόν, μια διαδικασία ανταλλαγής επιστολών και υπογραφή κάποιου συμφωνητικού μέσω fax ή ταχυδρομείου. Το θύμα έχει αρχίσει να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του χρηματικού ποσού. Στην πορεία και μετά από την αποστολή των χρημάτων από τη πλευρά του θύματος, θα διακοπεί η επικοινωνία με το δράστη. Υπάρχει επίσης και η περίπτωση που ο δράστης γνωρίζοντας τα στοιχεία της ταυτότητας του θύματος να χρεώνει τον τραπεζικό του λογαριασμό με υπέρογκα ποσά. Τα Νιγηριανά e-mail ονομάζονται επίσης “419” από το άρθρο του Νιγηριανού Ποινικού Κώδικα που παραβιάζουν.



2.1.8 ΕΠΙΘΕΣΕΙΣ ΑΡΝΗΣΗΣ ΕΞΥΠΗΡΕΤΗΣΗΣ

Οι επιθέσεις άρνησης εξυπηρέτησης έχουν ως στόχο την εισβολή σε ένα υπολογιστικό σύστημα με σκοπό την εξάντληση πόρων αυτού έτσι ώστε να μην μπορεί να εξυπηρετήσει άλλους υπολογιστές. Γενικότερα οι επιθέσεις αυτές έχουν σαν στόχο την παρεμπόδιση μετάδοσης δεδομένων στο δίκτυο, την παρεμπόδιση σύνδεσης σε υπηρεσίες, την αλλοίωση ποιότητας μιας υπηρεσίας που προσφέρεται στον χρήστη. Οι επιθέσεις άρνησης μπορούν να πραγματωθούν με τεχνικές όπως είναι οι τεχνικές επιθέσεις, SYN Flood Attacks, UDP Flood Attacks, ICMP Flood Attacks, Teardrop attacks, Ping of death, port flooding, OOB Attacks, Fragmentation, Smurf Attacks, Fraggle Attacks και Papasmurf Attacks. Οι πιο σημαντικές τεχνικές επιθέσεων είναι οι SYN Flood Attacks, Ping of death, Fragmentation.

Η εκτέλεση της επίθεσης άρνησης μπορεί να συνοψιστεί σε τέσσερα βασικά βήματα. Στο πρώτοβήμα ο εισβολέας εγκαθιστά το πρόγραμμα απομακρυσμένης διαχείρισης σε ηλεκτρονικούς υπολογιστές που διαθέτουν ευρυζωνικές συνδέσεις στο διαδίκτυο και στην πορεία γίνεται απόπειρα σύνδεσης με αυτούς τους υπολογιστές. Στο δεύτερο βήμα ο επιτιθέμενος δίνει εντολή στο πρόγραμμα να αποστείλει ping. Το ping είναι μια δικτυακή εφαρμογή μέσω της οποίας διαπιστώνεται αν μια διεύθυνση είναι προσβάσιμη. Ο υπολογιστής του δράστη λειτουργεί ως zombie, δηλαδή ο συγκεκριμένος υπολογιστής επιτρέπει στον επιτιθέμενο να το διαχειρίζεται από απόσταση. Στην τρίτη φάση πλέον έχουμε την ανταπόκριση του υπολογιστή – θύμα, ο όποιος απαντάει στα ping χωρίς όμως να μπορεί να πετύχει κάποια σύνδεση με τον υπολογιστή -zombie. Όσο ο υπολογιστής - θύμα περιμένει απάντηση, ο υπολογιστής - zombie συνεχίζει να στέλνει νέα ping. Το αποτέλεσμα είναι η άρνηση εξυπηρέτησης, δηλαδή οι πόροι του θύματος εξαντλούνται από την πληθώρα αιτημάτων κι έτσι είναι αδύνατη η προσφορά άλλων υπηρεσιών.

2.2 ΣΥΜΒΑΤΙΚΑ ΕΓΚΛΗΜΑΤΑ ΠΟΥ ΤΕΛΟΥΝΤΑΙ ΜΕ ΤΗ ΧΡΗΣΗ Η/Υ ΚΑΙ ΔΙΑΔΙΚΤΥΟΥ

Στη δεύτερη κατηγορία των βασικών μορφών ηλεκτρονικού εγκλήματος εντάσσονται τα εγκλήματα τα οποία παρόλο που προϋπήρχαν της εμφάνισης των ηλεκτρονικών υπολογιστών και του διαδικτύου, τα τελευταία συντελούν σε μεγάλο βαθμό στη διάπραξή τους. Πιο συγκεκριμένα ο υπολογιστής βοηθάει στην αποθήκευση προσωπικών δεδομένων και καταστάσεων παράνομων δραστηριοτήτων, στην εύρεση και εκμαίευση πληροφοριών παράνομων δραστηριοτήτων αλλά και στη διάδοση των πληροφοριών, ιδιαίτερα αν αυτές είναι συκοφαντικού περιεχομένου. Ακόμη ο υπολογιστής και το διαδίκτυο βοηθούν στην ηλεκτρονική αγορά με τη χρήση κλεμμένων πιστωτικών καρτών (που εκλάπησαν με φυσικό τρόπο) και στη διάδοση παράνομου οπτικοακουστικού υλικού όπως είναι η πορνογραφία

2.2.1 ΞΕΠΛΥΜΑ ΧΡΗΜΑΤΟΣ

Το ξέπλυμα χρήματος είναι η διαδικασία απόκρυψης χρημάτων που περιήλθαν στην κατοχή κάποιου με παράνομες διαδικασίες. Στην περίπτωση αυτή ο εγκληματίας

επιχειρεί τη μετατροπή των χρημάτων σε μια μορφή λιγότερο ύποπτη, στη συνέχεια το χρήμα διαχωρίζεται από την παράνομη πηγή του και διαχέεται σε διαφορές οικονομικές συναλλαγές με σκοπό την απόκρυψη του και τέλος ολοκληρώνεται η διαδικασία μετατροπής του παράνομου χρήματος σε ένα νόμιμο εισόδημα. Το διαδίκτυο κρατεί την ανωνυμία του πελάτη κι έτσι είναι δύσκολο να εντοπιστούν οι Κάτοχοι.

Η διαδικασία του ξεπλύματος διεθνώς έχει διαπιστωθεί ότι ακολουθεί τα παρακάτω τρία βασικά στάδια:

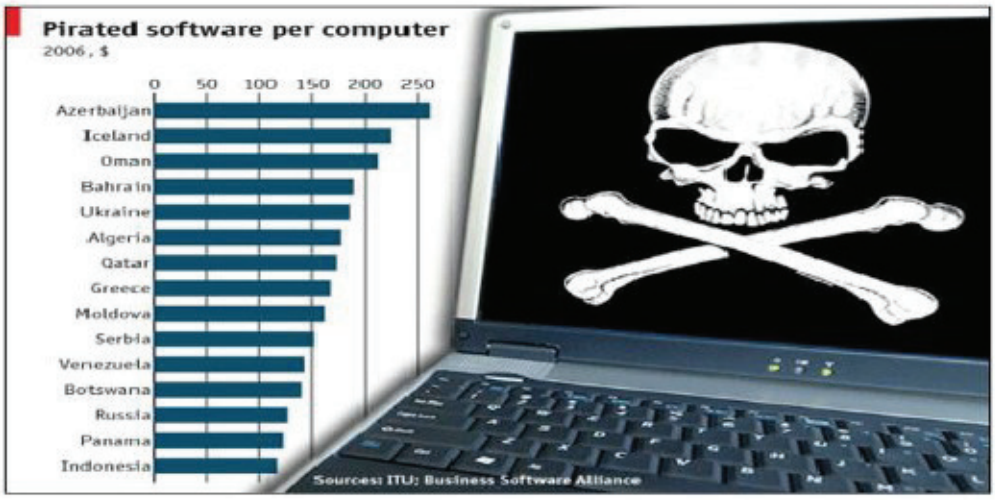
1. Τοποθέτηση : Ο δράστης τοποθετεί τα χρήματα που προέρχονται από παράνομη δραστηριότητα ως επένδυση στο γενικότερο οικονομικό σύστημα, σε παραδοσιακό ή μη χρηματοοικονομικό οργανισμό, όπως τράπεζα με κατάθεση σε λογαριασμό, χρηματιστήριο με αγορά μετοχών εισηγμένων σε αυτό, ανταλλακτήριο συναλλάγματος, καζίνο και άλλες συναφείς επενδύσεις.
2. Στρωματοποίηση : Ο δράστης επιχειρεί σειρά κινήσεων και συναλλαγών με αποκλειστικό σκοπό να απομακρύνει τα ίχνη των κεφαλαίων από την αρχική τους προέλευση και έτσι να μεταμφιέσει τις αληθινές πηγές κεφαλαίων, εμποδίζοντας τον εντοπισμό τους από τα ελεκτικά όργανα του φορέα στον οποίο επενδύθηκαν τελικά.
3. Ενσωμάτωση: Ο δράστης επανατοποθετεί τα κεφάλαια σε κλάδους νόμιμης οικονομικής δραστηριοτητας όπως για παράδειγμα σε αγορά ακινήτων, επιχειρηματικές και εμπορικές δραστηριότητες κλπ. Έτσι ώστε τα εν λόγω κεφάλαια να επιστρέφουν στο χρηματοοικονομικό σύστημα ως καθόλα νόμιμα κεφάλαια.

Η επανάσταση στην πληροφορική τεχνολογία έπαιξε καθοριστικό πόλο στην απόκρυψη αλλά και στη διακίνηση των οικονομικών προιόντων εγκληματικών ενεργειών. Έτσι λοιπόν,βλέπει κανείς ένα παραδοσιακό έγκλημα του ποινικού κώδικα να διαπράττεται με τη βοήθεια πλέον της τεχνολογίας και των νέων μέσων που αυτή προσφέρει , με σύγχρονους τρόπους και μεθόδους , όμως πάντα με τον ίδιο επιδιωκόμενο σκοπό.
Το βασικό πλεονέκτημα του ξεπλύματος χρήματος μέσω ίντερνετ είναι ότι δεν υπάρχει προσωπικ΄ή επαφή μεταξύ των συναλλασσομένων μερών με άμεσο επακόλουθο, οι δράστες να νοιώθουν μεγαλύτερη ασφάλεια και κρυμμένοι πίσω από

την ανωνυμία τους,να νομιμοποιούν έσοδα παράνομων δραστηριοτήτων. Όπως στην μεγάλη πλειοξηφία των εγκλημάτων του διαδικτύου, έτσι και στο ξέπλυμα χρήματος είναι εξαιρετικά δύσκολο να ανιχνευτεί, καθώς δεν υπάρχουν ακόμα οι κατάλληλοι μηχανισμοί εντοπισμού και ελέγχου.

2.2.2.ΠΕΡΑΤΕΙΑ ΛΟΓΙΣΜΙΚΟΥ

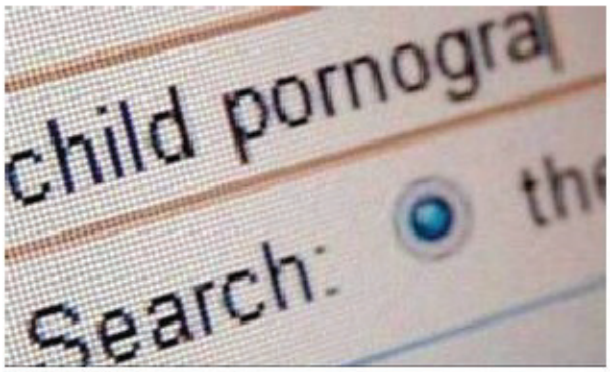
Αναφέρεται στην ηλεκτρονική μεταφορά προστατευομένου λογισμικού, απευθείας σε τρίτα άτομα χωρίς τη ρητή άδεια του δικαιούχου. Στο διαδίκτυο υπάρχουν πειρατικές ιστοσελίδες με παράνομα προγράμματα. Επιπλέον διακίνηση παράνομων προγραμμάτων γίνεται και μέσω των ηλεκτρονικών δημοπρασιών. Επενεργεί ανασταλτικά στην επένδυση κεφαλαίων από εθνικούς και ξένους επενδυτές σε παραγωγικό τομέα που τη σημερινή εποχή ανθεί σε παγκόσμιο επίπεδο και προσφέρει υψηλές υπηρεσίες. Στερεί τα κράτη από φορολογικούς πόρους αλλά και θέσεις απασχόλησης σε τομείς που σχετίζονται άμεσαή έμμεσα με την ανάπτυξη λογισμικού. Δημιουργεί μία ανεξέλεκτη παραοικονομία με υψηλά αφορολόγητα εισοδήματα. Κατ΄αρχήν ένα μεγάλο ποσοστό από την τιμή πώλησης κάθε προγράμματος διατίθεται για την έρευνα και την ανάπτυξη των προγραμμάτων. Συνεπως αγοράζοντας παράνομο λογισμικό πλουτίζουν οι πειρατές και μειώνονται οι επενδύσεις στη βελτίωση και ανάπτυξη νέου λογισμικού. Εκτός από τις εταιρίες παραγωγής λογισμικού, θίγεται όλος ο κάθετος κλάδος της εμπορίας, πώλησης και συντήρησης λογισμικού ανεξάρτητα από το μέγεθός τους.



Η πειρατεία λογισμικού εμποδίζει σημαντικά την ανάπτυξη των τοπικών βιομηχανιών λογισμικού. Εάν οι εκδότες λογισμικού δεν μπορούν να διαθέσουν τα προιόντα τους στη νόμιμη αγορά, δεν θα έχουν κίνητρο να συνεχίσουν να αναπτύ σουν τα προιόντα τους.Πολλοί εκδότες λογισμικού απλά δεν θα μπούν σε αγορές που σημειώνονται πολλά ποσοστά πειρατείας ,γιατί δεν θα μπορούν να καλύψουν τις ανάγκες τους για ανάπτυξη.

2.2.3 ΠΑΙΔΙΚΗ ΠΟΡΝΟΓΡΑΦΙΑ

Το φαινόμενο της πορνογραφίας ανηλίκων αποτελεί μάστιγα των σύγχρονων κοινωνιών σε παγκόσμιο επίπεδο και αποκτά ολοένα και μεγαλύτερες διαστάσεις με τους ταχύτατους ρυθμούς ανάπτυξης της τεχνολογίας. Η μεγέθυνση του κυβερνοχώρου παρέχει στους παραγωγούς και διακινητές του πορνογραφικού υλικού δυνατότητες γρήγορης και εύκολης προώθησης του παράνομου προιόντος τους. Οι εγκληματίες διακίνησης περνογραφικού υλικού ανηλίκων μέσα στον αχανή χώρο του διαδικτύου εξασφαλίζουν την ανωνυμία τους και δρουν ανενόχλητα εκμεταλλευόμενοι την παιδική αθωότητα.



Τι είναι όμως παιδική πορνογραφία; Σύμφωνα με το “Προαιρετικό Πρωτόκολλο της Σύμβασης για τα δικαιώματα του Παιδιού για την εμπορία παιδιών, την παιδική πορνεία και την παιδική πορνογραφία “ και συγκεκριμένα στο άρθρο 2 “παιδική περνογραφία σημαίνει οποιαδήποτε αντιπροσώπευση, με οποιαδήποτε μέσα, ενός παιδιού που συμμετέχει σε πραγματικές ή προσωμοιωμένες, ρητές σεξουαλικές δραστηριότητες ή οποιαδήποτε αντιπροσώπευση των σεξουαλικών μελών ενός παιδιού για πρώτιστα σεξουαλικούς σκοπούς”.
Άν και το φαινόμενο της παιδικής πορνογραφίας προυπήρχε των ηλεκτρονικών υπολογιστών και του διαδικτύου, ο κυβερνοχώρος φαίνεται να εξελίσσεται σε κυρίαρχο μέσο διανομής του πορνογραφικού υλικού.
Με τη χρήση του διαδικτύου:
1. Εξασφαλίζεται μυστικότητα και ανωνυμία που βοηθά το χρήστη-εγκληματία να αποκρύψει την ταυτοτητά του
2. Υπάρχει προσβασιμότητα του επίμαχου υλικού ανα πάσα στιγμή από χρήστες ολόκληρης της υφηλίου με μικρό σχετικά κόστος
3. Οι παιδόφιλοι έχουν τη δυνατότητα να παρακολουθούν σε πραγματικό χρόνο τη σεξουαλική κακοποίηση ανηλίκων
4. Διευκολύνεται η ανταλλαγή πορνογραφικού υλικού (ταινίες, φωτογραφίες κλπ) το οποίο μέσα σε λίγα λεπτά μπορεί να κυκλοφορήσει σε έναν μεγάλο αριθμό χρηστών μέσω ηλεκτρονικού ταχυδρομείου.
Μια ολόκληρη βιομηχανία πορνό έχει αναπτυχθεί στο ίντερνετ με θύματα εκατομμύρια ανηλίκους.Η πορνογραφία στο ίντερνετ σήμερα βρίσκεται στα χέρια επιχειρηματιών. Πρόκειται για sites που μοιάζουν απόλυτα με εμπορικά sites τα οποία πουλάνε διάφορα άλλα είδη , όπως λόγου χάρη βιβλία, είδη ένδυσης ,σπιτιού κλπ..

Δεν υπάρχει ιδιαίτερη δυσκολία να βρεθεί ο χρήστης του διαδικτύου μπροστά σε ένα παρνογραφικό site, εφόσον οι διαφημίσεις τους είναι πολλές και εμφανίζονται με τη μορφή banner ακόμη και σε μια “αθώα” περιήγηση στο ίντερνετ. Η παιδική περνογραφία στο διαδίκτυο αποτελεί στη σύγχρονη εποχή μια άριστα οργανωμένη “επιχειρηματική” δραστηριότητα. Αποτελεί προιόν μιας επικερδέστατης επιχείρησης καθώς οι χρήστες που επιθυμούν να αποκτήσουν πρόσβαση σε πορνογραφικό υλικό ανηλίκων που παρέχουν διάφορες ιστοσελίδες καταβάλουν διόλου ευκαταφρόνητα ποσά.

Οι επιπτώσεις σε βάρος των ανηλίκων, μπορούν να ειδωθούν από πολλές οπτικές γωνίες. Οι ανήλικοι μετατρέπονται σε θύματα των ενηλίκων , αποφέροντάς τους ιδιαίτερα υψηλά κέρδη, εφόσον μετατρέπονται σε εμπορεύσιμα είδη υψηλής αξίας. Επιπλέον μετατρέπονται σε “μέσα” ικανοποίησης των σεξουαλικών τους ορέξεων. Όμως υπάρχει και ένας άλλος κίνδυνος για τους ανηλίκους , που δεν είναι τόσο φανερός όσο οι προηγούμενοι, αλλά που είναι όμως εξίσου σοβαρός και ικανός να προκαλέσει ανεπανόρθωτες βλάβες, κυρίως ως προς τη σεξουαλική του ωρίμανση. Ο ανήλικος από την πλευρά του , είναι ικανότατος χρήστης των υπολογισών και συνήθης επισκέπτης του διαδικτύου. Εξαιτίας λοιπόν κάποιων φυσικών γνωρισμάτων του νεαρού της ηλικίας του, όπως της έντονης περιέργειας και του ατίθασου χαρακτήρα του ,μπορεί εύκολα να πέσει στις παγίδες του διαδικτύου. Έτσι μπορεί εύκολα ένας ανήλικος να γίνει ο ίδιος καταναλωτής του πορνογραφικού υλικού ή ακόμα να συμμετέχει στην παραγωγή του, πειθόμενος από αυτούς που γνώρισε δια μέσω του ιστού.
Οι παιδόφιλοι χρησιμοποιούν το διαδίκτυο για τις δραστηριότητέςτους μέσω συστημάτων που προωθούν την επικοινωνία και τις συζητήσεις σεξουαλικού περιεχομένου ή ακόμα και μέσω δικτύων ανταλλαγής υλικού. Επίσης και μέσω ιστοσελίδων που διαφημίζουν διάφορες μορφές πορνογραφικού υλικού (εικόνες, βίντεο, κλπ).

Πίνακας 2.1: Μορφές πορνογραφικού υλικού

ΑΠΕΙΚΟΝΙΣΕΙΣ ΑΝΗΛΙΚΩΝ	ΠΕΡΙΓΡΑΦΗ
Ενδεικτικές	Μη ερωτικές ή μη σεξουαλικής φύσης φωτογραφίες που απεικονίζουν ανήλικους με τα εσώρουχα τους,μαγιό κλπ συγκεντρωμένες από νόμιμες πηγές(περιοδικά, διαφημιστικούς καταλόγους κλπ)
Γυμνισμού	Γυμνές ή ημίγυμνες φωτογραφίες ανηλίκων που έχουν συλλαχθεί από νόμιμες πηγές
Ερωτικές	Φωτογραφίες ανήλικων τραβηψμένες κρυφά μα εσώρουχα ή με άλλες μορφές γυμνισμού (πχ Θάλασσα)
Πόζες	Φωτογραφίες ανήλικων γυμνών ή ημίγυμνων σκοπίμως τραβηγμένες
Ερωτικές πόζες	Φωτογραφίες ανήλικων γυμνών ή ημίγυμνων σκοπίμως τραβηγμένες σε σεξουαλικές πόζες
Ερωτικών στάσεων	Φωτογραφίες ανήλικων γυμνών ή ημίγυμνων σκοπίμως τραβηγμένες με έμφαση στα γεννητικά όργανα.
Ερωτικής δραστηριότητας	Απεικόνιση κάθε μορφής σεξουαλικής δραστηριότητας μεταξύ ανηλίκων (χωρίς τη συμμετοχή ενήλικα)
Επιθετικές	Απεικονίσεις ανηλίκων που δέχονται σεξουαλική κακοποίηση από ενήλικα και οι οποίες καταλήγουν σε ολοκληρωμένη σεξουαλική πράξη
Σαδισμού/κτηνοβασίας	Απεικονίσεις ανηλίκων οι οποίοι υπόκεινται σε σωματικό πόνο ή συμμετέχουν σε σεξουαλικές δραστηριότητες με ζώα.

Με βάση το άρθρο 348Α του Ποινικού Κώδικα , οι τρόποι εγκλεξματικής δράσης είναι:
1.Κατασκευή υλικού πορνογραφίας (κινηματογραφική λήψη,μοντάζ, επεξεργασία εικόνων κλπ)
2.Κατοχή πορνογραφικού υλικού δηλαδή φυσική εξουσίαση επί του υλικού
3.Προμήθεια και αγορά υλικού (πραγματική μετακίνηση του πορνογραφικού υλικού στην κατοχή του δράστη)
4.Μεταφορά του πορνογραφικού υλικού
5.Κυκλοφορία πορνογραφικού υλικού (διακίνηση, διάθεση, πώληση)

Έχουμε λοιπόν δύο μορφές της παιδικής πορνογραφίας στο διαδίκτυο:από τη μία τη βιομηχανοποιημένη δημιουργία και διακίνηση πορνογραφικού υλικού με στόχο την πραγματοποίηση κέρδους και από την άλλη την ατομοκεντρική εκδοχή προς ικανοποίηση της προσωπικής διαστροφής του δράστη.

2.2.4 ΔΙΑΔΙΚΤΥΑΚΗ ΤΡΟΜΟΚΡΑΤΙΑ

Τα τελευταία χρόνια η χρήση του διαδικτύου αποτελεί έργαλείο των τρομοκρατών.Το FBI ορίζει την κυβερνοτρομοκρατία (cyber terrorism) ως την προσχεδιασμένη ,πολιτικά υποκινούμενη επίθεση εναντίον πληροφοριών, υπολογιστικών συστημάτων,προγραμμάτων ηλεκτρονικών υπολογιστών και δεδομένων που καταλήγουν στην άσκηση βίας έναντι αμάχων στόχων από υποεθνικές ομάδες και μυστικούς πράκτορες.

Οι τρομοκράτες με τη χρήση του διαδικτύου απολαμβάνουν μια σειρά από πλεονεκτήματα: Είναι φθηνότερο σε σχέση με τις άλλες τρομοκρατικές μεθόδους και οι ενέργειες τους δύσκολα εντοπίζονται. Ακόμα,μπορούν να εξαπολύσουν την επίθεση τους από οποιοδήποτε σημείο του κόσμου και να επιτεθούν ταυτόχρονα σε πολλούς στόχους. Όσον αφορά το θέμα της ανωνυμίας, το διαδίκτυο είναι ένας χώρος όπου προς το παρόν τουλάχιστον υπάρχει ελευθερία της έκφρασης και αυτή μπορεί να ενθαρρύνει κάποιον να μεταδώσει αυτά που θέλει,διατηρώντας την ανωνυμία του.Με τη χρήση λοιπόν του διαδικτύου οι τρομοκράτες μπορούν να παρακάμψουν τις ασφαλιστικές δικλείδες στις οποίες υπόκεινται τα παραδοσιακά ΜΜΕ και να έχουν παγκόσμια πρόσβαση σε εκατοντάδες εκατομμύρια ανθρώπων.Είναι προφανές ότι υπάρχει μια νέα γενιά τρομοκρατών με σύγχρονη μόρφωση που γνωρίζει ότι μεταδίδοντας πληροφορίες με το κατάλληλο ύφος και στον κατάλληλο χρόνο, μπορεί να επιφέρει πρακτικά, σπουδαία στρατηγικά αποτελέσματα. Ένα παράδειγμα είναι η οργάνωση Al-Kaida ,η παγκόσμια τρομοκρατική απειλή που αναπτύσσοντας ένα

ευρύτατο δίκτυο επικοινωνίας με τη χρήση του διαδικτύου κατάφερε να συντονίσει άψογα τις ενέργειες της στο χτύπημα των δίδυμων πύργων της 11ης Σεπτεμβρίου 2001. Επίσης το 1999 ένας δεκαεπτάχρονος Αμερικανός που λειτουργούσε με το όνομα Chameleon βρέθηκε να κλέβει δορυφορικές εικόνες από τις στρατιωτικές ιστοσελίδες των Η.Π.Α. Ο Chameleon θεωρήθηκε ότι βρισκόταν στην υπηρεσία του Osama Bin Laden, ο άνθρωπος που ήταν ύποπτος ότι βρίσκεται πίσω από τον βομβαρδισμό των Αμερικάνικων βάσεων στην Ανατολική Αφρική το 1998 και συνεπώς στην κορυφή των καταζητουμένων του FBI.
Το 1998 οι Tamil Guerrilas πλημμύρισαν τις βάσεις της Sri Lanka με ηλεκτρονικά μηνύματα στέλνοντας περίπου 800 την ημέρα για μια περίοδο δύο εβδομάδων. Στόχος τους ήταν να διακόψουν την ικανότητα επικοινωνίας και το περιστατικό αυτό είναι το πρώτο γνωστό περιστατικό τρομοκρατικής επίθεσης εναντίον των ηλεκτρονικών συστημάτων μιας χώρας,

Μ Ε Ρ Ο Σ 2ο

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

ΚΕΦΑΛΑΙΟ 3

Το διαδίκτυο έχει γίνει πλέον αναπόσπαστο κομμάτι των εξελιγμένων κοινωνιών. Αποτελεί εξαιρετικό βοήθημα του ανθρώπου στον τομέα της επιστήμης, της εκπαίδευσης, του εμπορίου, της ψυχαγωγίας. Ωστόσο το ερώτημα που τίθεται είναι κατά πόσο ασφαλές μπορεί να είναι το διαδίκτυο. Πόσο ασφαλή είναι τα δεδομένα που καταθέτουμε σε αυτό; Αρχικά θα πρέπει να δοθεί ο ορισμός της έννοιας «ασφάλεια».
Ο όρος ασφάλεια στον τομέα των πληροφοριακών συστημάτων σχετίζεται με την ικανότητα ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του (Πάγκαλος, 2000).
Η ασφάλεια των συστημάτων έχει να κάνει με :
- Τη πρόληψη μη εξουσιοδοτημένων ενεργειών έναντι ενός συστήματος.
- Την ανίχνευση κάθε είδους επίθεσης.
- Την αντίδραση, δηλαδή τη λήψη μέτρων για την αποκατάσταση της ζημιάς που προκλήθηκε από τον επιτιθέμενο.

Τα τρία παραπάνω στοιχεία συνθέτουν την πολιτική ασφάλειας ενός οργανισμού και καθορίζει τις διαδικασίες που ακολουθούνται για την αντιμετώπιση των απειλών.

3.1 ΒΑΣΙΚΟΙ ΟΡΟΙ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι βασικές έννοιες της ασφάλειας είναι η εμπιστευτικότητα (confidentiality), η ακεραιότητα (integrity), η διαθεσιμότητα (availability).

Με το όρο εμπιστευτικότητα εννοούμε την προστασία των δεδομένων από άτομα που δεν έχουν καμία εξουσιοδότηση για πρόσβαση σε αυτά τα δεδομένα. Εμπιστευτικότητα δεν θα πρέπει να υπάρχει μόνο στα ίδια τα δεδομένα αλλά και στην

ύπαρξη τους. Πρόκειται δηλαδή για απόλυτη μυστικότητα.

Με την έννοια της ακεραιότητας εννοείται η απόλυτη (ακέραιη) διατήρηση των πληροφοριών και η μη εξουσιοδοτημένη μεταβολή τους. Η αποφυγή κάθε είδους παραποίησης ή αλλοίωσης.

Τέλος, με τη διαθεσιμότητα εννοούμε την δυνατότητα εκμαίευσης πληροφοριών χωρίς δυσκολίες και καθυστερήσεις ενός πληροφοριακού συστήματος. Η απειλή στη διαθεσιμότητα είναι η άρνηση εξυπηρέτησης.

3.2 ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ & ΠΡΟΛΗΨΗ

Η πρόληψη αποτελεί το βασικότερο παράγοντα στο πληροφοριακό σύστημα ενός οργανισμού μιας και αποτελεί την απαρχή της ασφάλειας του συστήματος.

3.2.1 ΔΙΑΔΙΚΑΣΙΕΣ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

Η αυθεντικοποίηση είναι εκείνη που θα εμποδίσει την οποιαδήποτε μη εξουσιοδοτημένη παρέμβαση και είναι απλά η διαδικασία της «ταυτοπροσωπίας». Η επιβεβαίωση της ταυτότητας ενός πρόσωπου μπορεί να γίνει είτε με τους κωδικούς πρόσβασης – ασφάλειας, είτε με τα φυσικά χαρακτηριστικά του χρήστη π.χ. δακτυλικά αποτυπώματα, είτε με κάτι που ο χρήστης θα έχειστην κατοχή του όπως είναι μια έξυπνη κάρτα.
Τα παραπάνω αποτελούν στοιχεία πιστοποίησης ταυτότητας αλλά δεν σημαίνει ότι είναι απόλυτα ασφαλή, με εξαίρεση τα φυσικά χαρακτηριστικά. Για το λόγο αυτό, όταν η ασφάλεια ενός συστήματος επείγει, απαιτείται ένα πιο σύνθετο σύστημα τεχνικής της ασφάλειας.

Κωδικοί πρόσβασης

Οι κωδικοί πρόσβασης λόγω της απλότητάς τους έχουν γίνει πλέον από τους πιο διαδεδομένους τρόπους προστασίας δεδομένων, αφού αρκεί μόνο η εισαγωγή του username και του κωδικού που είναι ξεχωριστοί κάθε φορά για τον καθένα. Είναι εύκολο να απομνημονευτούν αλλά και να αλλαχτούν από τον ίδιο τον χρηστή όταν

αυτό είναι απαραίτητο. Όπως όμως αναφέρθηκε και προηγουμένως ακόμα και αυτή η μέθοδος είναι αμφιλεγόμενη αφού η αποκάλυψη ενός κωδικού πρόσβασης πλέον είναι πολύ εύκολη και απλή διαδικασία. Αρκεί μονό η εφαρμογή απλών εργαλείων λογισμικού.

Σε πολλά συστήματα από αυτά που χρησιμοποιεί ο χρηστής οι κωδικοί πρόσβασης καθορίζονται από τον ίδιο και μπορούν να αντικατασταθούν κάθε στιγμή. Συνήθως ο χρήστης επιλεγεί κωδικούς που είναι εύκολο να απομνημονευτούν και που σημαίνουν κάτι για αυτόν όπως είναι η ημερομηνία γέννησης, το τηλέφωνό του κ.α. όμως αυτούς τους κωδικούς είναι εύκολο για κάποιον να τους μαντέψει. Σε κάποιες άλλες περιπτώσεις οι κωδικοί πρόσβασης δίνονται από τους ίδιους τους διαχειριστές του συστήματος και αυτό καθιστά πιο δύσκολη την απόσπασή τους από άλλους.

Αρκετές φορές ένας υπάλληλος μπορεί να αποκαλύψει τον κωδικό πρόσβασης σε έναν συνάδελφο για δική του εξυπηρέτηση κι ο δεύτερος υπάλληλος σε κάποιον άλλον κι έτσι έχουμε το διαμοιρασμό αυτού του κωδικού με αποτέλεσμα να παύει η μυστικότητά του.
Επιπλέον η παρακολούθηση των πακέτων που διακινούνται στο δίκτυο μπορεί να έχει σαναποτέλεσμα την ανάκτηση κωδικών πρόσβασης. Στη σύνδεση ενός απομακρυσμένου υπολογιστή με τον κεντρικό, απαιτείται η εισαγωγή του κωδικού πρόσβασης, ο όποιος θα διακινηθεί μέσω του υπολογιστή.
Τέλος, ένας κωδικός πρόσβασης αποθηκεύεται σε ένα αρχείο του διακομιστή όπου και γίνεται η ταυτοποίηση. Σε περίπτωση που το αρχείο δεν φυλάσσεται επαρκώς ο εισβολέας μπορεί να ανακτήσει τον κωδικό αυτό.\

Βιομετρικές τεχνικές

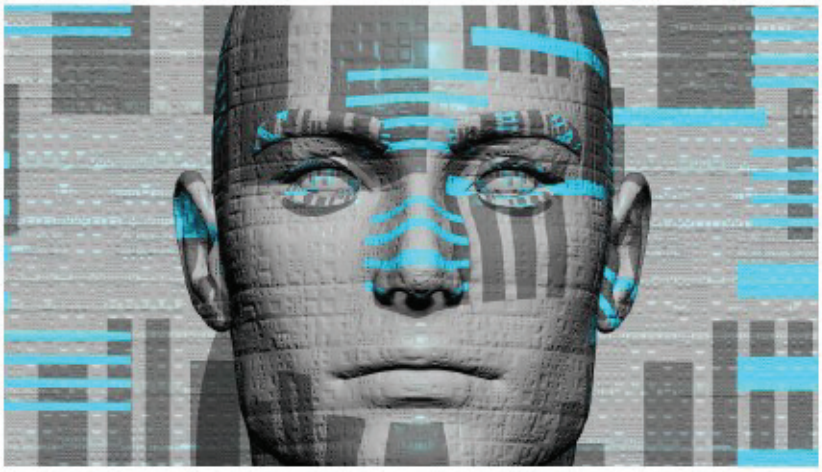
Με τον όρο βιομετρία εννοούμε την επιστήμη η οποία χρησιμοποιεί ψηφιακή τεχνολογία για την ταυτοποίηση των ατόμων. Θεωρείται αρκετά ασφαλή μέθοδος προστασίας των δεδομένων και στοχεύει στη επαλήθευση και στην επιβεβαίωση της ταυτότητας ενός χρηστή με βάση μοναδικά χαρακτηριστικά.
Στις βιομετρικές τεχνικές εντάσσονται:

Σάρωση δακτυλικού αποτυπώματος

Το δακτυλικό αποτύπωμα είναι ένα χαρακτηριστικό σχεδόν μοναδικό σε κάθε άτομο

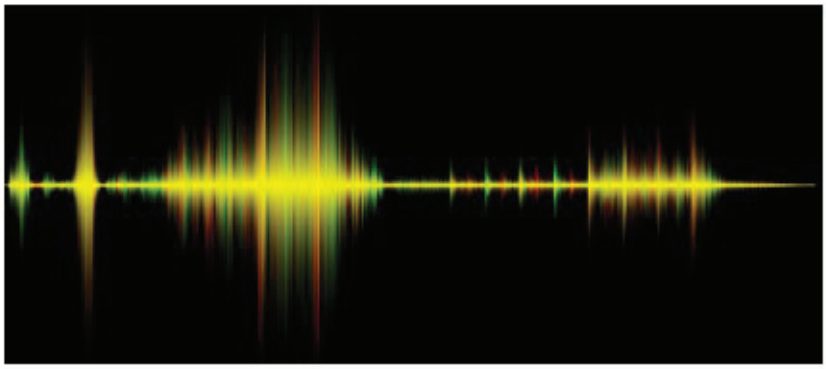
(αφού έχει διαπιστωθεί πως η πιθανότητα ύπαρξης πανομοιότυπου αποτυπώματος σε άλλο πρόσωπο είναι μία στο δισεκατομμύριο) και άρα αποτελεί αξιόπιστη μέθοδος ταυτοποίησης. Η λήψη των αποτυπωμάτων γίνεται με οπτικούς αναγνώστες, με υπέρυθρες ακτίνες και τεχνολογίες σιλικόνης.

Αναγνώριση προσώπου



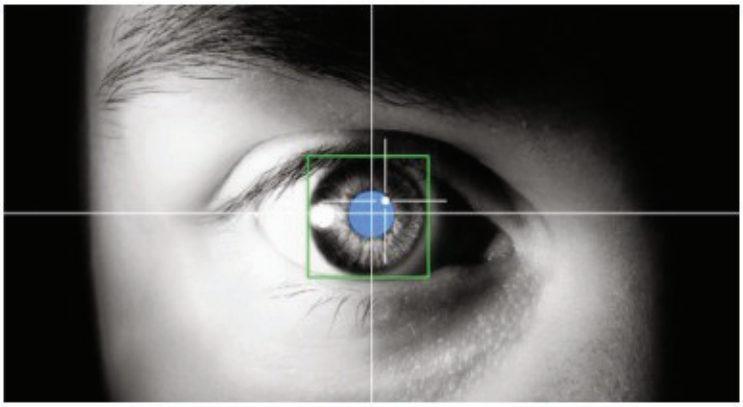
Η αναγνώριση του πρόσωπου (face recognition) αποτελεί μια βιομετρική τεχνική που βασίζεται στα χαρακτηριστικά του πρόσωπου του χρηστή. Δίνεται έμφαση σε σημεία του πρόσωπου που είναι λιγότερο ευάλωτα στην αλλαγή, όπως είναι το περίγραμμα του ματιού, η όψη του στόματος και οι αποστάσεις μεταξύ των ματιών του στόματος και των φρυδιών. Είναι ευνόητο πως κάτι τέτοιο δεν είναι πάντα πρακτικό και πολλά συστήματα αντιμετωπίζουν δυσκολία στο να πετύχουν μεγάλα επίπεδα απόδοσης.

Σάρωση φωνής



Σε αυτή τη βιομετρική τεχνική γίνεται η ταυτοποίηση – σάρωση της φωνής του χρήστη, αναγνωρίζοντας το μοναδικό ηχητικό σήμα που αυτός δίνει με μια φράση λέξη -κλειδί. Στην εν λόγω τεχνική το σύστημα μπορεί να κάνει την ταυτοποίηση και εξ’αποστασεως. Αυτό σημαίνει ότι δεν είναι απαραίτητη η φυσική παρουσία του άτομου αλλά μπορεί να βρίσκεται σε απόσταση χρησιμοποιώντας το τηλέφωνο του ή ένα κοινό μικρόφωνο.

Σάρωση ίριδας και αμφιβληστροειδή χιτώνα



Η ίριδα είναι το έγχρωμο μέρος που περιβάλλει την κόρη του ματιού και διαθέτει 250 χαρακτηριστικά και το κάθε ένα από αυτά είναι μοναδικά σε κάθε άτομο. Η πιθανότητα να ταιριάξει απόλυτα ο γενετικός κώδικας της ίριδας του χρηστή με το γενετικό κώδικα κάποιου αλλού είναι μηδαμινή. Επομένως, η αναγνώριση της ίριδας θεωρείται απόλυτα αξιόπιστη μέθοδος.
Εξίσου αξιόπιστη μέθοδος είναι και η σάρωση του αμφιβληστροειδή χιτώνα. Ο αμφιβληστροειδήςχιτώνας είναι μοναδικός σε κάθε άνθρωπο και παραμένει ίδιος καθ' όλη τη διάρκεια της ζωής, με εξαίρεση κάποιων σοβαρών ασθενειών του ματιού. Η τεχνική αυτή όμως θεωρείται δύσχρηστη.

Σάρωση χεριού

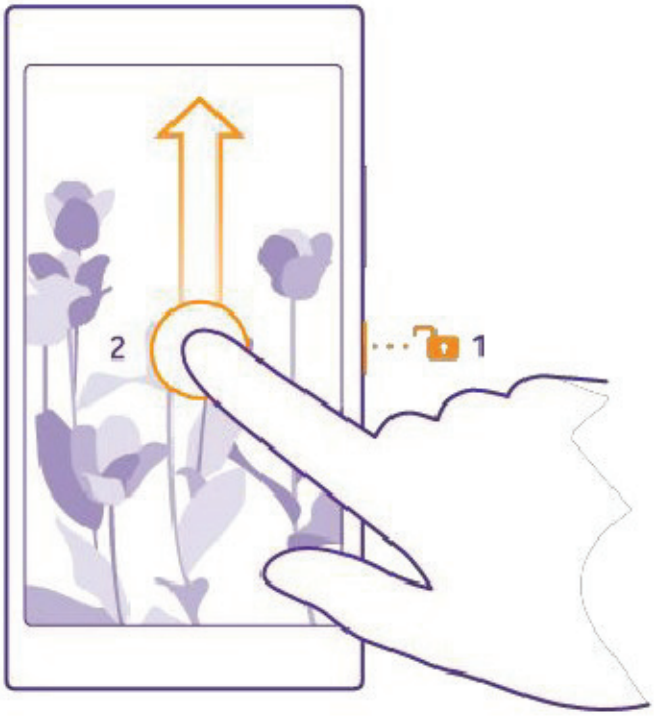
Η τεχνική της σάρωσης του χεριού είναι παρόμοια με εκείνη του πρόσωπου αφού και σε αυτή τη περίπτωση αναγνωρίζονται στοιχεία του χεριού όπως είναι το μήκος των δακτύλων, η απόσταση μεταξύ των κλειδώσεων και το σχήμα των αρθρώσεων. Με αυτό το τρόπο πετυχαίνεται η ταυτοποίηση του χρήστη. Η σάρωση χεριού δεν είναι

αρκετά ακριβής τεχνολογία, ωστόσο χρησιμοποιείται για εφαρμογές χαμηλού επιπέδου ασφάλειας.

Σάρωση υπογραφής

Η σάρωση υπογραφής βασίζεται στη μοναδικότητα και στην αυθεντικότητα της υπογραφής. Ενώ θα μπορούσε να θεωρηθεί αμφιλεγόμενη η αξιοπιστία του λόγο της πλαστογραφίας, η βιομετρική αυτή τεχνολογία είναι αρκετά ασφαλής. Η αξιοπιστία του συστήματος έγκειται στο ότι αναγνωρίζεται η ταχύτητα, η πίεση και η δύναμη του νόμιμου χρήστη. Ωστόσο, η σάρωση της υπογραφής δεν χρησιμοποιείται ακόμα ευρέως αλλά σίγουρα στο μέλλον θα φάνει χρήσιμος σύμβουλος για την πιστοποίηση αυθεντικότητας επίσημων εγγράφων.

Σάρωση πατήματος πλήκτρου



Η δυναμική πατήματος πλήκτρου (keystroke dynamics) είναι η αναγνώριση δακτυλογράφησης και βασίζεται στα χαρακτηριστικά του τρόπου πληκτρολόγησης του χρηστή. Τα χαρακτηριστικά αυτά είναι η ταχύτητα, η δύναμη, η συχνότητα λάθους, ο χρόνος δακτυλογράφησης ενός συγκεκριμένουσυνθηματικού, αλλά και ο χρόνος που μεσολαβεί από το πάτημα ενός συγκεκριμένου πλήκτρου έως το πάτημα του επόμενου.

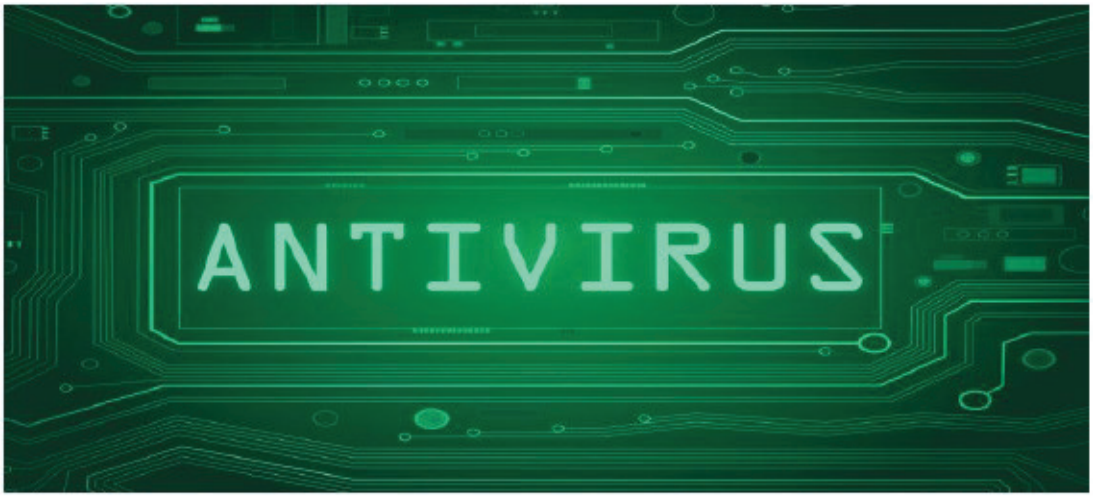
Πολλές από τις προαναφερόμενες τεχνικές φαντάζουν πρωτόγνωρες, μερικές αρκετά αξιόπιστεςκαι άλλες λιγότερο. Κοινό χαρακτηριστικό τους είναι ότι βασίζονται όχι σε αριθμούς – κωδικούς ενός χρήστη αλλά στα ίδια τα χαρακτηριστικά του. Τα χαρακτηριστικά του ανθρώπου είναιμοναδικά και δε μπορούν να παραβιαστούν ή να

υποκλαπούν και για τον λόγο αυτό η βιομετρική τεχνολογία αναπτύσσει περισσότερες τέτοιες τεχνικές. Μερικές από αυτές είναι η ταυτοποίηση με βάση το σχήμα του αυτιού, την οσμή, τη σάρωση της φλέβας, τη γεωμετρία του δακτύλου, τη σάρωση νυχιού και την αναγνώριση βηματισμού.

3.2.2 ΧΡΗΣΗ ΛΟΓΙΣΜΙΚΟΥ ΑΣΦΑΛΕΙΑΣ

Στα μέτρα πρόληψης θα πρέπει να συμπεριληφθεί η δημιουργία λογισμικού ασφάλειας. Τα antivirus και τα firewalls είναι οι πιο διαδεδομένες εφαρμογές και στη συνεχεία θα γίνει διεξοδική αναφορά σε αυτές.

Antivirus



Οι ιοί είναι η πιο γνωστή και διαδεδομένη μορφή επίθεσης. Υπάρχουν ιοί που μπορούν να προκαλέσουν μεγάλη και ανεπανόρθωτη ζημία, αλλά υπάρχουν και ιοί που είναι λιγότερο ζημιογόνοι. Σε κάθε περίπτωση η εγκατάσταση λογισμικού ασφάλειας είναι απαραίτητη σε κάθε υπολογιστικό σύστημα. Η δημιουργία του λογισμικού antivirus έπεται της δημιουργίας κάθε νέου ιού έτσι ώστε να μπορέσει να προσφέρει την ανάλογη ασφάλεια. Οι ιοί δημιουργούνται και μεταδίδονται μαζικά καθημερινά απειλώντας τα υπολογιστικά συστήματα. Ποια είναι όμως η λειτουργία των αντιβιοτικών; Ένα τέτοιο λογισμικό δρα σε τρία στάδια:

- Η ανίχνευση των ιών είναι η πρώτη και βασική λειτουργία. Μέσα από την ανίχνευση το λογισμικό επιβεβαιώνει την τυχούσα μόλυνση. Η ανίχνευση είναι μια λειτουργία που είτε δρα έπειτα από επιθυμία του χρηστή, είτε αυτόματα, κάτι το οποίο συμβαίνει με τα σύγχρονα υπολογιστικά συστήματα.
- Ο προσδιορισμός της ταυτότητας των ιών είναι το επόμενο στάδιο μετά την ανίχνευση κατά το οποίο το λογισμικό ενημερώνει για τον τύπο του ιού που μόλυνε το σύστημα. Η ταυτότητα του ιού μας δείχνει το μέγεθος της ζημιάς που έχει προκληθεί αλλά και τη δυνατότητα ανασυγκρότησης του συστήματος.
- Ο καθαρισμός τω ιών είναι η τελευταία λειτουργία του λογισμικού κι εντοπίζει

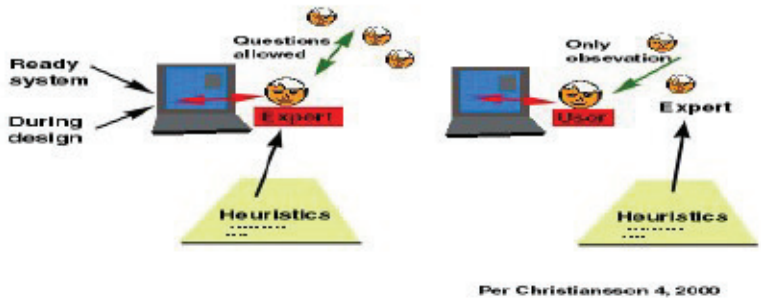
τα αρχεία στα οποία βρίσκεται ο ιός. Η πλειοψηφία των λογισμικών προτείνουν στον χρήστη να επιδιορθώσει ή και να διαγράψει το αρχείο που μολύνθηκε από τον ιό ή ακόμα και να το θέσει σε καραντίνα ώστε να μην μπορεί να χρησιμοποιηθεί.

Ο χρήστης κατά την εγκατάσταση του αντιβιοτικού έχει μια βασική προστασία. Όμως, όπως ήδη ειπώθηκε, δημιουργούνται χιλιάδες ιοί καθημερινά οι οποίοι απειλούν τα υπολογιστικά συστήματα και για αυτό οι εταιρείες λογισμικού δίνουν τη δυνατότητα στο χρηστή για on-line ενημέρωση της βάσης δεδομένων του προγράμματος με τους νέους ιούς.
Ο εντοπισμός του κάθε ιού γίνεται με βάση του μοναδικού χαρακτηριστικού στοιχείου του, που ονομάζεται αποτύπωμα ή υπογραφή. Σε ένα σύστημα αντιβιοτικού τα αποτυπώματα αυτά είναι αποθηκευμένα σε μια λίστα. Όταν λοιπόν, κατά τη σάρωση που θα τελέσει το πρόγραμμα ανιχνεύσει υπογραφή όμοια με αυτή που έχει αποθηκεύσει, τότε ειδοποιεί το χρήστηγια τη μόλυνση που έχει υποστεί το σύστημα του και στη συνέχεια ακολουθεί η παραπάνω διαδικασία.

Έτσι προκύπτει το συμπέρασμα πως για να εντοπιστεί μια υπογραφή θα πρέπει να είναι καταχωρημένη στη βάση δεδομένων του προγράμματος του λογισμικού. Με την εμφάνιση ενός ιού ενημερώνεται και η βάση δεδομένων από τις εταιρίες σε ένα αρκετά γρήγορο χρονικό διάστημα.
Ωστόσο μεσολαβεί το χρονικό διάστημα από την εμφάνιση του ιού σε αρκετές χιλιάδες υπολογιστές μέχρι την ενημέρωση των βάσεων δεδομένων των προγραμμάτων των εταιρειών.
Αυτό το χρονικό διάστημα προσπαθούν να αντιμετωπίσουν οι εταιρείες με νέες τεχνικές και μεθόδους.

Οι σχετικές τεχνολογίες που τυγχάνουν ευρείας ανάπτυξης τα τελευταία χρόνια είναι η ευρετική ανάλυση και ο έλεγχος ακεραιότητας.

Ευρετική Ανάλυση (heuristic):



Στην ευρετική ανάλυση το πρόγραμμα λογισμικού ασφάλειας δεν αναζητεί τις υπογραφές των ιών για να τις ταιριάξει με αυτές των βάσεων δεδομένων του προγράμματος, αλλά ελέγχει τα αρχεία τα οποία εκτελεί ο υπολογιστής και κατόπιν προσπαθεί να προσδιορίσει αν στον κώδικά τους περιέχονται εντολές οι οποίες να προέρχονται από ιούς. Η επιτυχία αυτού του προγράμματος ανέρχεται στο 60% με

90%. Το σημαντικό σε αυτή την εφαρμογή antivirus είναι ότι δεν χρειάζεται να ενημερώνεται η βάση δεδομένων του προγράμματος. Έτσι, δεν μεσολαβεί χρόνος μεταξύ της παρουσίας του ιού και του χρόνου καταγραφής του στο πρόγραμμα, που είναι και το ζητούμενο.

Έλεγχος Ακεραιότητας (Integrity Check):

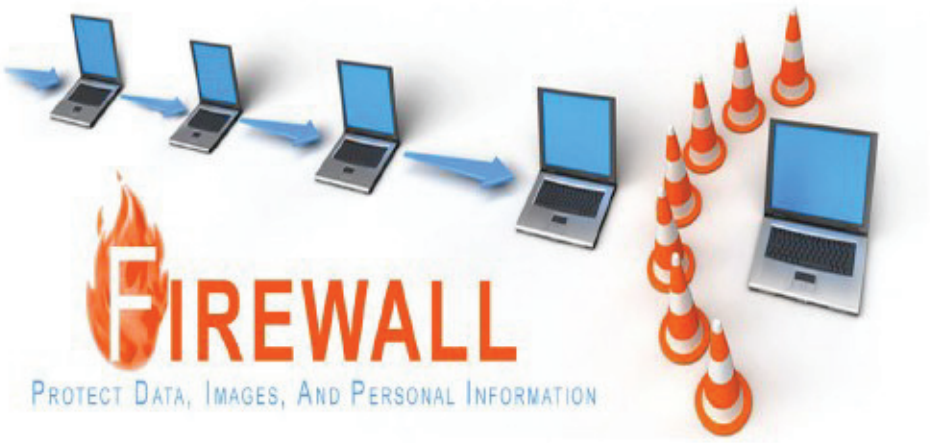
Ο έλεγχος ακεραιότητας είναι μια τεχνική για την ανίχνευση των ιών χωρίς όμως να δίνει την ταυτότητα αυτών. Ο έλεγχος εκτελείται σε δύο φάσεις:
Στην πρώτη φάση, για κάθε αρχείο που βρίσκεται στο σύστημα υπολογίζεται ένα ~~άθροισμα έλεγχου. Το άθροισμα αυτό είναι ένας αριθμός μοναδικός για κάθε αρχείο,~~ ενώ ακόμα και η ελάχιστη τροποποίηση που θα υφίσταται το αρχείο θα μεταβάλει το άθροισμα αυτό, το οποίο και θα αποθηκεύεται σε μια βάση δεδομένων.
Στη δεύτερη φάση τα αθροίσματα αυτά θα υπολογίζονται εκ νέου και θα συγκρίνονται με τα περιεχόμενα της βάσης δεδομένων. Σε περίπτωση που θα ~~παρατηρηθεί διαφορά θα σημαίνει ότι υπάρχει πιθανή παρουσία ιού. Τα δύο~~ αυτά προγράμματα φέρουν καλύτερα αποτελέσματα όταν δουλεύουν συνδυαστικά.

Κριτήρια επιλογής λογισμικού ανίχνευσης ιών

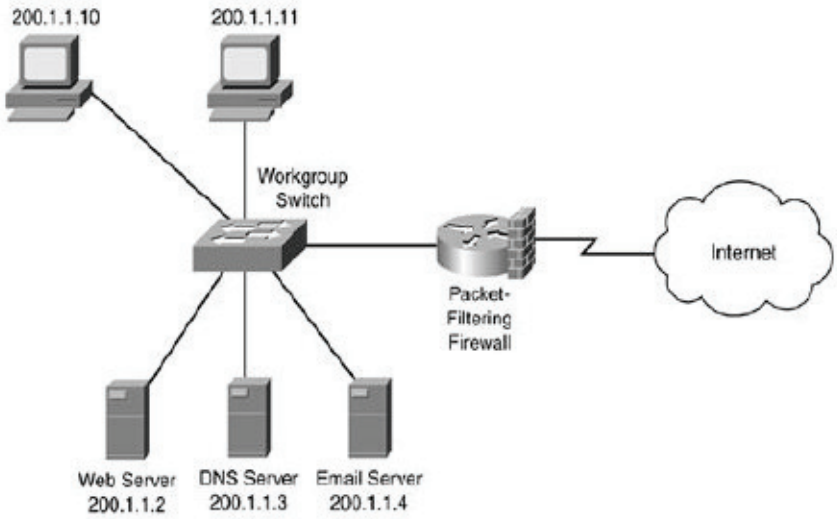
Στην παγκόσμια αγορά κυκλοφορούν πολλά λογισμικά ανίχνευσης ιών. Επομένως για την επιλογή του λογισμικού θα πρέπει να λαμβάνονται υπόψη κάποια συγκεκριμένα κριτήρια –προϋποθέσεις. Οι βασικότερες προϋποθέσεις είναι :

- Εύχρηστο interface και χαμηλή κατανάλωση πόρων
- Προστασία σε πραγματικό χρόνο
- Αυτόματη ενημέρωση
- Προστασία ηλεκτρονικής αλληλογραφίας
- Προγραμματισμένος έλεγχος
- Δισκέτα εκκίνησης
- Καταγραφή συμβάντων
- Firewalls

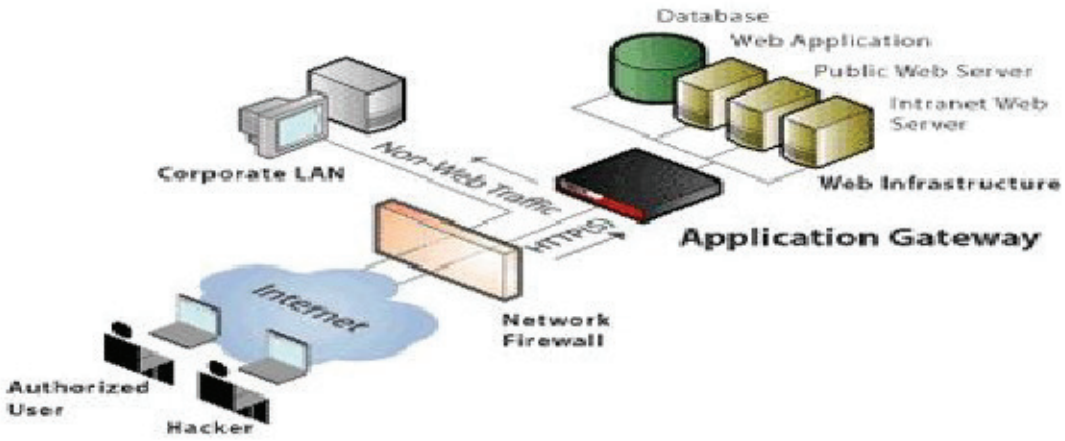
Με τον όρο firewall εννοείται ένα τοίχος προστασίας.



Ο όρος αυτός χρησιμοποιήθηκε για πρώτη φορά από τις τεχνικές εταιρείες για να προσδιορίσουν το τοίχος που χώριζε δυο σημεία με σκοπό να μην επεκταθεί η φωτιά σε περίπτωση πυρκαγιάς. Αντίστοιχη έννοια είχε και στην περιγραφή των περιβλημάτων στα ντεπόζιτα καύσιμων των αγωνιστικών αυτοκίνητων, τα οποία εμπόδιζαν τη διείσδυση της φωτιάς στα καύσιμα.
Παρόμοια έννοια έχει και στην επιστήμη των υπολογιστών αφού σαν firewall προσδιορίζεται μια συσκευή ή εργαλείο λογισμικού που παρακολουθεί και φιλτράρει τα πακέτα που επιχειρούν να εισέλθουν ή να εξέλθουν από ένα εσωτερικό προστατευμένο δίκτυο ή υπολογιστή. Ουσιαστικά είναι ένα τείχος που προστατεύει ένα ασφαλές εσωτερικό «χώρο» από ένα μη ασφαλές εξωτερικό, όπως είναι το διαδίκτυο.
Δυο είναι οι βασικές λειτουργίες ασφάλειας που επιτελούν τα firewalls και είναι οι ακόλουθες:
Φιλτράρισμα πακέτων (packet filtering), όπου με τη διαδικασία αυτή επιτρέπεται ή απαγορεύεται αντίστοιχα ηκίνηση των πακέτων που διακινούνται στο δίκτυο σύμφωνα με την πολιτική ασφάλειας του οργανισμού.



Πύλες εφαρμογών (application proxy gateways), όπου προσφέρονται υπηρεσίες στους εσωτερικούς χρήστες και ταυτόχρονα προστατεύονται οι hosts από εξωτερικές απειλές.



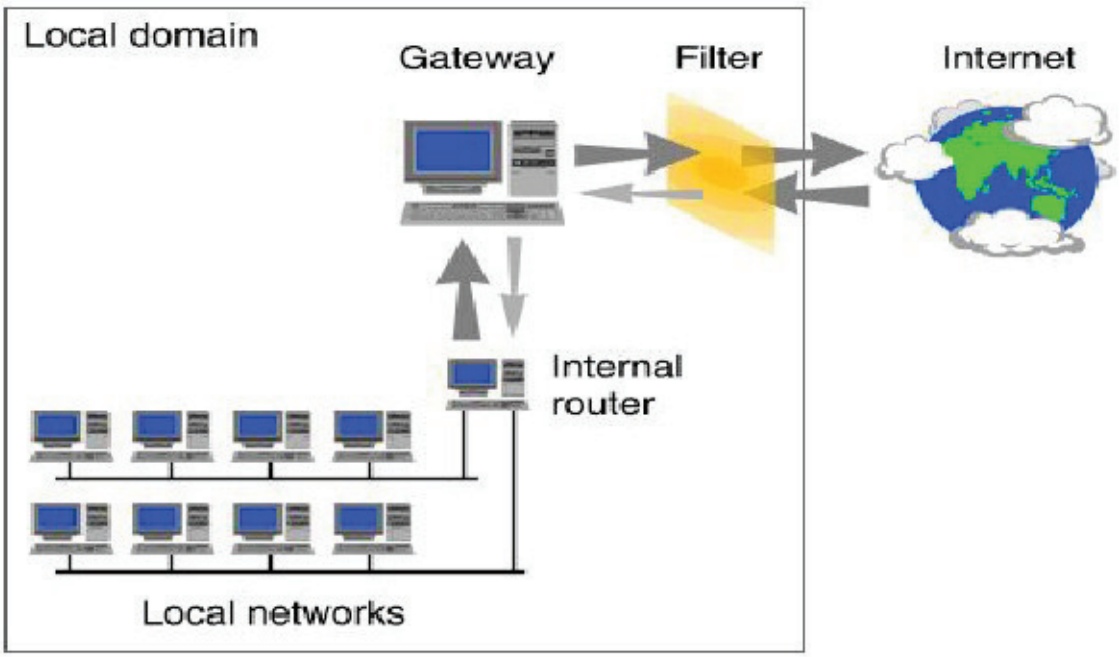
Η λειτουργία που θα επιτελέσει το firewall έχει να κάνει με την πολιτική ασφάλειας που ακολουθείο οργανισμός. Οι πολιτικές ασφάλειας είναι δύο και είναι οι ακόλουθες:

- Πολιτική προκαθορισμένης άδειας χρήσης (allow-everything-not-specifically-denied), όπου η κυκλοφορία πακέτων και η εκτέλεση εφαρμογών είναι ελεύθερη, εκτός από περιπτώσεις στις οποίες υπάρχει ρητή απαγόρευση.

- Πολιτική προκαθορισμένης απαγόρευσης χρήσης (deny-everything-not-specifically-allowed), στην οποία το firewall δεν επιτρέπει καμία κυκλοφορία πακέτων και καμία εκτέλεση εφαρμογής, εφόσον δεν έχουν καθοριστεί εκ των πρότερων. Η ασφάλεια σαφέστατα σε αυτή τη περίπτωση είναι μεγαλύτερη σε σχέση με την πρώτη, από την άλλη πλευρά όμως είναι μια λειτουργία που θα δυσανασχετήσει τους χρήστες.

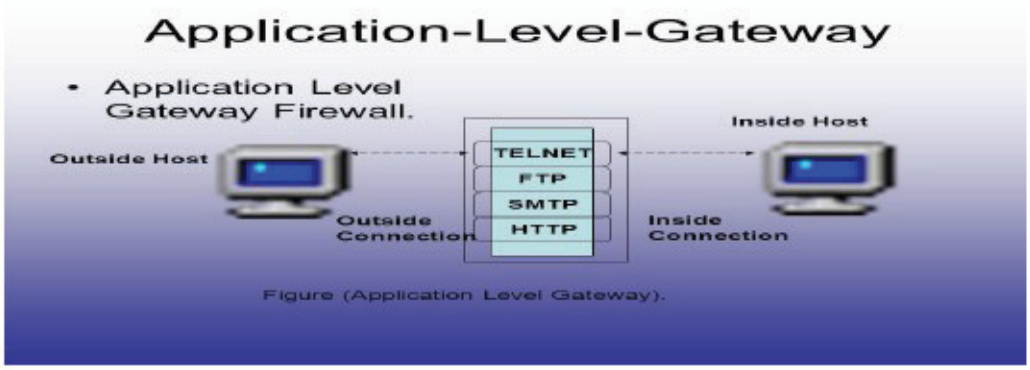
Σήμερα που το ηλεκτρονικό έγκλημα έχει πάρει τεράστιες διαστάσεις, η χρήση των firewalls είναι επιτακτική ανάγκη. Η τεχνολογία στον τομέα αυτό βελτιώνεται συνεχώς παρέχοντας στο χρήστη μεγαλύτερη ασφάλεια και προστασία, προσφέροντας firewalls ικανά να επιτελούν πολλές εργασίες ταυτόχρονα. Σε μια προσπάθεια διαχωρισμού των firewalls, μπορούμε να διακρίνουμε τρεις βασικές τεχνικές προστασίας:

Πύλες φιλτραρίσματος:



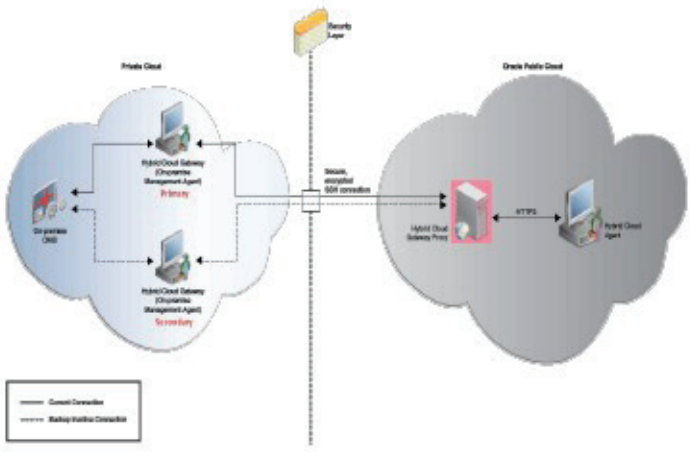
Οι πύλες φιλτραρίσματος πακέτων (Packet filtering gateways) είναι η πιο απλή διαδικασία των firewalls. Τα πακέτα που διακινούνται στη δίκτυο και διέρχονται από τα firewalls φιλτράρονται με βάση κάποιους προκαθορισμένους κανόνες που θέτει ο ίδιος ο διαχειριστής. Το πακέτο που θα διαπεραστεί είτε θα απορριφτεί είτε θα γίνει αποδεκτό. Τα κριτήρια που θα επιτρέψουν ή θα απαγορεύσουν την διέλευση του πακέτου είναι:
α) η διεύθυνσηIP του αποστολέα και του παραλήπτη, με δυνατότητα ομαδοποίησης των διευθύνσεων με τη χρήση μάσκας,
β) η θυρίδα προέλευσης και προορισμού και
γ) το χρησιμοποιούμενο πρωτόκολλο επικοινωνίας.
Το αδύνατο σημείο στις πύλες φιλτραρίσματος είναι ότι στις διευθύνσεις IP δεν εξετάζεται το περιεχόμενο αλλά μόνο οι IP επικεφαλίδες από τις οποίες λαμβάνονται οι πληροφορίες δρομολόγησης και στη συνέχεια γίνεται η αξιολόγηση για αποδοχή ή απόρριψη.

Πύλες εφαρμογών:



Οι πύλες εφαρμογών (application gateways) δρουν σε επίπεδο εφαρμογής. Βασικό χαρακτηριστικό είναι η ύπαρξη μιας υπηρεσίας διαμεσολάβησης, που πραγματώνεται με τη χρήση ενός πακέτου λογισμικού proxy server. Αυτό το πακέτο λογισμικού λειτουργεί ταυτόχρονα σαν πελάτης και σαν διακομιστής, δηλαδή στους εσωτερικούς χρήστες παίρνει το ρόλο του διακομιστή, ενώ για τους εξωτερικούς χρήστες παίρνει το ρόλο του πελάτη. Η υπηρεσία proxy έχει τη δυνατότητα να παρεμβάλλεται μεταξύ των πρωτοκόλλων επικοινωνίας κι έτσι έχει τον έλεγχο των επικοινωνιών. Όταν ένας εξωτερικός χρήστης επιθυμεί πρόσβαση σε μια υπηρεσία του προστατευόμενου δικτυού, θα πρέπει πρώτα να συνδεθεί με την proxy εφαρμογή όπου θα γίνει η αναγνώριση και πιστοποίησή του και στη συνέχεια θα του επιτραπεί η πρόσβαση στη ζητούμενη υπηρεσία. Έτσι οι πύλες ελέγχουν το περιεχόμενο των πακέτων που δρομολογούνται αποτρέποντας επιθέσεις IP και DNS spoofing. Οι πύλες εφαρμογών μπορεί να υπερτερούν σε αυτό το χαρακτηριστικό σε σχέση με τις πύλες φιλτραρίσματος αλλά υστερούν σε ταχύτητα.

Υβριδικές πύλες:



Οι υβριδικές πύλες (hybrid gateways) είναι μια τεχνική που συνδυάζει την ταχύτητα των πυλών φιλτραρίσματος και την αξιοπιστία των πυλών εφαρμογών με συνέπεια τα υβριδικά firewalls να είναι τα επικρατέστερα. Η πιο εξελιγμένη μορφή των υβριδικών firewalls, Stateful Inspection, συμπληρώνει το IP - φιλτράρισμα από μια υπηρεσία ελέγχου του εσωτερικού των πακέτων λαμβάνοντας υπόψη προηγούμενες επικοινωνίες. Αυτές οι πληροφορίες αποθηκεύονται σε μια βάση δεδομένων η οποία ανανεώνεται συνεχώς και η σύγκριση των δεδομένων με τα πακέτα που εισέρχονται των firewalls επιτρέπει ή απορρίπτει αντίστοιχα την Επικοινωνία.

3.2.3 ΚΡΥΠΤΟΓΡΑΦΙΑ

Η κρυπτογραφία (cryptography) είναι μια μέθοδος που συναντάμε από την αρχαιότητα, όπου η κρυπτογράφηση γινόταν με τη χρήση κωδικών - συμβόλων. Το

κάθε σύμβολο αντιστοιχούσε σε ένα γράμμα της αλφαβήτου. Η κρυπτογραφία αποτελεί μέρος του κλάδου της κρυπτολογίας.
Σύμφωνα με τον ορισμό που δίνεται από την Wikipedia είναι η επιστήμη που ασχολείται με τους μαθηματικούς μετασχηματισμούς για την εξασφάλιση της ασφάλειας της πληροφορίας. Η κρυπτανάλυση από την άλλη πλευρά είναι ο κλάδος που αναλαμβάνει την αποκρυπτογράφηση, δηλαδή η ανάλυση και το σπάσιμο των αλγορίθμων της κρυπτογράφησης. Με τηνκρυπτογράφηση επιτυγχάνεται η εμπιστευτικότητα (confidentiality), η ακεραιότητα (integrity), η αυθεντικοποίηση (authentication) και η μη αποποίηση παραλαβής – αποστολής (non repudiation).
Στην κρυπτογράφηση γίνεται η μετατροπή της πληροφορίας από μια κατανοητή μορφή σε ένανγρίφο – κωδικό. Η διαδικασία που θα μετατρέψει αυτό τον γρίφο στην αρχική του κατανοητή μορφή είναι η αποκρυπτογράφηση.

Για τη διαδικασία αυτή απαιτούνται τέσσερα βασικά στοιχεία:
α) το αρχικό μήνυμα,
β) το κρυπτογραφικό σύστημα που θα αποτελείται από ένα αλγόριθμο κρυπτογράφησης κι ένα αλγόριθμο αποκρυπτογράφησης,
γ) το κρυπτογραφημένο κείμενο που θα προέρχεται από την εφαρμογή του αλγορίθμου κρυπτογράφησης στο αρχικό μήνυμα, πριν αυτό σταλεί στον παραλήπτη και
δ) ένα κλειδί που αποτελείται από μια συμβολοσειρά, που χρησιμοποιείται από τους αλγορίθμους στη διαδικασία κρυπτογράφησης και αποκρυπτογράφησης.
Η κρυπτογραφία διακρίνεται σε δυο βασικές κατηγορίες:

Τη συμμετρική κρυπτογραφία (symmetric cryptography), στην οποία υπάρχει ένα ιδιωτικό κλειδί και την ασύμμετρη κρυπτογραφία (asymmetric cryptography), στην οποία έχουμε ένα ιδιωτικό κι ένα δημόσιο κλειδί.
Το κύριο χαρακτηριστικό της συμμετρικής κρυπτογραφίας είναι ότι υπάρχει ένα μόνο κλειδί που κρυπτογραφεί και αποκρυπτογραφεί. Ο αποστολέας κρυπτογραφεί το μήνυμα με το κλειδί και αποστέλλει το κρυπτογραφημένο πλέον μήνυμα στον παραλήπτη μέσω ενος καναλιού επικοινωνίας. Ο παραλήπτης παραλαμβάνει το μήνυμα το οποίο και αποκρυπτογραφεί με τηχρήση του ίδιου του κλειδιού. Βασικό είναι το κλειδί να δίνεται στον ενδιαφερόμενο μέσα από ασφαλείς διαύλους επικοινωνίας.

Η ασύμμετρη κρυπτογραφία είναι πιο ασφαλής μέθοδος από τη συμμετρική λόγω της ύπαρξης δύο κλειδιών. Το ένα κλειδί ονομάζεται δημόσιο επειδή είναι γνωστό σε όλους και χρησιμοποιείται για την κρυπτογράφηση του μηνύματος. Το δεύτερο κλειδί ονομάζεται ιδιωτικό και είναι γνωστό μονό σε αυτόν που θα κάνει την αποκρυπτογράφηση. Αν και τα δυο αυτά κλειδιά συσχετίζονται μεταξύ τους, η γνώση του ενός δε μπορεί να οδηγήσει στην αποκάλυψη του αλλού.
Από τη στιγμή που τα κλειδιά είναι δύο δεν απαιτείται η ύπαρξη ασφαλούς δίαυλου επικοινωνίας για την ανταλλαγή τους.
Στην ασύμμετρη κρυπτογράφηση όταν ένας χρήστης θέλει να λάβει ένα

κρυπτογραφημένο μήνυμα, δίνει στον αποστολέα το δημόσιο κλειδί του, με το όποιο γίνεται η κρυπτογράφηση του μηνύματος. Η αποκρυπτογράφηση γίνεται με τη χρήση του ιδιωτικού κλειδιού που έχει μόνο αυτός. Αυτή η διαδικασία ωστόσο απαιτεί μεγαλύτερα κλειδιά από αυτά που απαιτεί η συμμετρική.
Αδύνατα σημεία συναντώνται και στις δύο περιπτώσεις. Στη πρώτη περίπτωση το πρόβλημα είναι η εύρεση ενός καναλιού επικοινωνίας που θα παρέχει τη μέγιστη ασφάλεια και στη δεύτερη περίπτωση απαιτούνται πολύ μεγαλύτερα κλειδιά για την αποκρυπτογράφηση, κάτι που καθιστά την διαδικασία χρονοβόρα. Τη λύση σε αυτά τα προβλήματα έρχεται να δώσει το υβριδικό σύστημα κρυπτογράφησης.
Το υβριδικό σύστημα κρυπτογράφησης είναι ένας συνδυασμός των δύο παραπάνω. Χρησιμοποιείται η ασύμμετρη κρυπτογραφία για την ανταλλαγή του μυστικού κλειδιού. Όταν η ανταλλαγή του μυστικού κλειδιού ολοκληρωθεί το παραλαμβάνουν οι χρήστες μέσω ασφαλούς καναλιού επικοινωνίας. Η επικοινωνία πραγματοποιείται με τη συμμετρική κρυπτογράφηση των δεδομένων.
Ένα πρόβλημα το όποιο γεννάται έχει να κάνει με την πιστοποίηση αυθεντικότητας των δημοσίων κλειδιών. Η εξακρίβωση αυτή είναι πολύ σημαντική γιατί κατά την επαλήθευση μιας ψηφιακής υπογραφής ο χρηστής πρέπει να είναι βέβαιος ότι το δημόσιο κλειδί που χρησιμοποιεί για την επαλήθευση είναι πραγματικά το κλειδί του υπογράφοντος. Ως ακολούθως απαιτείται η συνεχής εξακρίβωση από τον ίδιο τον χρηστή. Σε αυτό το σημείο έρχεται να βοηθήσει η αρχή πιστοποίησης. Η αρχή πιστοποίησης παρέχει τη δυνατότητα διακρίβωσης για τα δημόσια κλειδιά. Υπογράφει με το δικό της ιδιωτικό κλειδί τα δημόσια κλειδιά και τα αντίστοιχα ονόματα προσθέτοντας κάποια επιπλέον στοιχεία. Το κομμάτι των δεδομένων που έχει υπογραφεί από την αρχή πιστοποίησης ονομάζεται πιστοποιητικό και μπορεί να επαληθευτεί με το δημόσιο κλειδί της αρχής πιστοποίησης.
Ακόμα και στην κρυπτογράφηση δεν λείπει η απειλή της επίθεσης η οποία ελλοχεύει στην κρυπτανάλυση. Οι μέθοδοι και οι τεχνικές τις κρυπτανάλυσης αποτελούν τα βασικά εργαλεία των επιτιθέμενων έναντι αυτών της κρυπτογράφησης. Σημαντικό ρόλο σε αυτή την επίθεση κατέχει το υλικό το οποίο χρησιμοποιεί ο δράστης. Στην περίπτωση κατά την οποία ο επιτιθέμενος έχει στην κατοχή του ένα κρυπτογραφημένο υλικό τότε η πιθανότητα αποκωδικοποίησης είναι απειροελάχιστη. Εάν όμως μαζί με το κρυπτογραφημένο υλικό έχει και το αντίστοιχο αρχικό τότε είναι πολύ εύκολο να βρει το κλειδί. Για να βρεθεί το αντίστοιχο κλειδί απαιτείται μεγάληπροσπάθεια και αρκετός χρόνος, κάτι που καθίστα το σύστημα ασφαλέστερο. Οι αλγόριθμοι είναι αρκετά δύσκολο να σπάσουν όχι όμως ακατόρθωτο, αφού αν κάποιος διαθέσει χρόνο δοκιμάζοντας όλα τα πιθανά κλειδιά, μπορεί να οδηγηθεί στο σωστό. Ωστόσο η μεγάλη δαπάνη χρόνου αρκεί για να αποτρέψει τον δράστη από αυτή τη διαδικασία.

3.2.4 ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

Η φυσική ασφάλεια είναι ένας από τους σημαντικότερους τομείς στους οποίους θα πρέπει να δώσει σημασία ένας χρήστης ή ένας οργανισμός. Είναι μια σκέψη την οποία παραμελούν αρκετοί δίνοντας βαρύτητα στην προστασία του συστήματος με

σύγχρονο και εξελιγμένο λογισμικό. Η ύπαρξη ενός άριστου λογισμικού δεν έχει κανένα νόημα από τη στιγμή που κάποιος θα μπορέσει να φτάσει στην φυσική τοποθεσία όπου φυλάσσεται ο υπολογιστής και να αφαιρέσει το σκληρό δίσκο. Στη φυσική ασφάλεια θα πρέπει να συμπεριλάβουμε όλα εκείνα τα μετρά που θα προφυλάξουν τον υπολογιστή όχι μονό από μια ενδεχόμενη επίθεση ενός εγκληματία αλλά και από όλες εκείνες τις ζημιές που μπορούν να προκληθούν και από φυσικά αίτια, όπως είναι οι πλημμύρες, η φωτιά, ο σεισμός. Απαιτείται ο εξοπλισμός του κτιρίου με συστήματα πυρόσβεσης, με αντισεισμικά μετρά και γενικότερα με κατασκευές υψίστης ασφαλείας.
Πολλές φορές καλώδια δικτύων, διακομιστές, δρομολογητές και άλλες συσκευές βρίσκονται εκτιθέμενα μεγαλώνοντας τον κίνδυνο για απευθείας παρέμβαση, η οποία μπορεί να στοχεύει στην καταστροφή του δικτυού, στην παρεμβολή συσκευών η ακόμα και στην υποκλοπή δεδομένων. Επίσης, μεγάλη προσοχή και προστασία θα πρέπει να δοθεί στις αποθηκευτικές μονάδες, μέσα στις οποίες μπορεί να υπάρχουν δεδομένα που περιέχουν σημαντικές πληροφορίες για την ασφάλεια του συστήματος. Την φυσική προστασία των υπολογιστικών συστημάτων έρχονται να βοηθήσουν και οι βιομετρικές τεχνολογίες. Η φυσική πρόσβαση δηλαδή, θα πρέπει να επιτυγχάνεται με μεθόδους όπως είναι η φωνητική αναγνώριση, η σάρωση της ίριδας ή το δακτυλικό αποτύπωμα.

3.3 ΑΝΙΧΝΕΥΣΗ ΕΠΙΘΕΣΕΩΝ

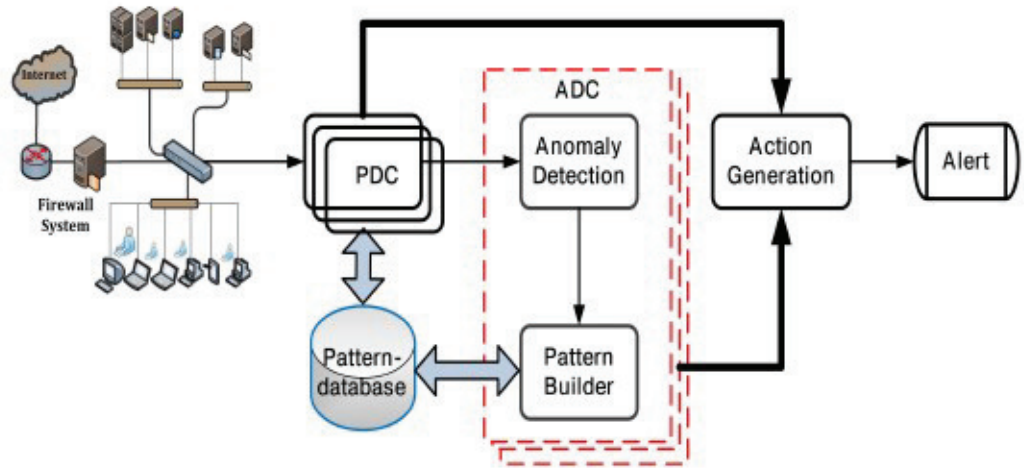
Τα μέτρα πρόληψης, στα οποία έγινε διεξοδική αναφορά, είναι η βασική συνιστώσα της ασφάλειας του πληροφοριακού συστήματος ενός οργανισμού. Στην περίπτωση όμως που ο επιτιθέμενος καταφέρει να εισβάλει στο σύστημα, τότε αυτό θα πρέπει να εντοπίσει την επίθεση το συντομότερο δυνατό προκειμένου να την αποτρέψει και να αποκαταστήσει τις τυχόν ζημιές.

3.3.1 ΣΥΣΤΗΜΑ ΑΝΙΧΝΕΥΣΗΣ ΕΠΙΘΕΣΕΩΝ

Το Σύστημα Ανίχνευσης Επιθέσεων είναι από τις βασικότερες λειτουργίες αφού εντοπίζει οποιαδήποτε προσπάθεια μη εξουσιοδοτημένης πρόσβασης στο δίκτυο και τοποθετείται από τονδιαχειριστή. Υπάρχουν τρία μοντέλα ανίχνευσης επιθέσεων:

Ανίχνευση ανωμαλιών
Ανίχνευση υπογραφών
Υβριδικό μοντέλο

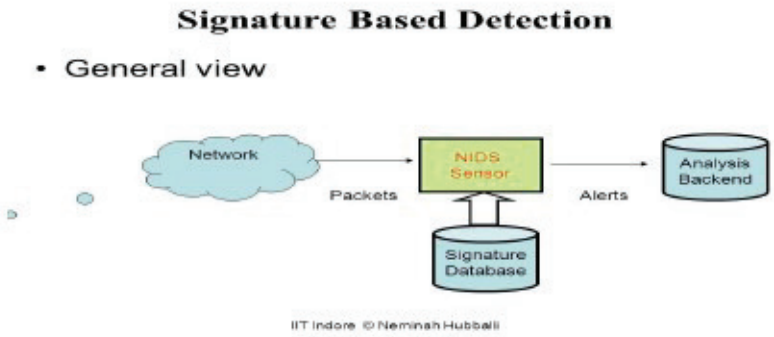
Ανίχνευση Ανωμαλιών (anomaly-based detection)



General architecture of the intelligent IDS IntErA

Η ανίχνευση ανωμαλιών είναι ένα σύστημα το οποίο λειτουργεί με μια μέθοδο αυτοεκπαίδευσης.
Καταγράφει λοιπόν τις ροές και τις διαδικασίες δεδομένων προσπαθώντας να κάνει ένα είδος τυποποίησης. Οι τυποποιημένες αυτές διαδικασίες βοηθάνε στον εντοπισμό ανωμαλιών που πιθανόν να αποτελούν εισβολή σύμφωνα με όσα έχουν ήδη καταγραφεί. Ωστόσο, είναι πιθανόντο σύστημα να αναγνωρίσει σαν εισβολή μια διαδικασία – κίνηση που έχει νόμιμη χρήση. Για να καταγράψουν το γνωστικό τους περιεχόμενο, οι διαδικασίες αυτές, χρησιμοποιούν ευρετικές μεθόδους αξιοποιώντας με στατιστικά κριτήρια τα δεδομένα του συστήματος. Επομένως υπάρχει ο κίνδυνος σε περίπτωση που τα συστήματα δεν έχουν ρυθμιστεί καλά, να δίνουν λανθασμένες εντολές, δηλαδή να δίνουν λάθος συναγερμούς ή αντίθετα να μην αναγνωρίζουν – εντοπίζουν μια επίθεση.

Ανίχνευση Υπογραφών (signature-based detection)



Η ανίχνευση υπογράφων είναι μια μέθοδος παρόμοια με εκείνη που χρησιμοποιούν τα λογισμικά συστήματα antivirus για την ταυτοποίηση και τον εντοπισμό ενός ιού. Τα συστήματα ανίχνευσης υπογραφών στηρίζονται στο γεγονός ότι για κάθε επίθεση υφίσταται μία και μοναδική υπογραφή.
Αυτή η υπογραφή λοιπόν αποθηκεύεται στη βάση δεδομένων στην οποία θα γίνεται και η σύγκριση. Ακόμα κι αν υπάρχει μικρή απόκλιση μεταξύ των δυο υπογραφών ο εντοπισμός είναι εφικτός. Παρόλα αυτά και σε αυτή τη περίπτωση απαιτείται η συνεχής ενημέρωση της βάσης.

Υβριδικό μοντέλο (hybrid detection)

Το υβριδικό μοντέλο έρχεται να συμπληρώσει τα δυο προηγούμενα μοντέλα κάνοντας ένανσυνδυασμό των προτερημάτων τους. Η τεχνολογία των υβριδικών μοντέλων βρίσκεται σε πρώιμο στάδιο και διαχωρίζεται στα συστήματα που συλλέγουν πληροφορίες 1) από το δίκτυο 2) από τους υπολογιστές και 3) από εφαρμογές.
Τα εν λόγω συστήματα θυμίζουν τη λειτουργία των firewalls αφού κι αυτά παρακολουθούν την κίνηση στο δίκτυο με σκοπό να εντοπίσουν τυχόν επιθέσεις. Επίσης είναι υπεύθυνα για τον εντοπισμό ανωμαλιών, δυσλειτουργιών καθώς και δεδομένων που πιθανόν να είναι κακόβουλα ή επιβλαβή. Σε αντίθεση όμως με τα firewalls είναι διακριτικά και δεν αντιλαμβάνεται την παρουσίατους ο επιτιθέμενος αφού δεν επεμβαίνουν στο δίκτυο για να διακόψουν ή να αλλοιώσουν την κίνηση.
Το συγκεκριμένο σύστημα ανίχνευσης εστιάζει στις απειλές που προέρχονται από το εσωτερικό μιας εταιρίας αφού όπως έχει ηδη τονισθεί, οι απειλές δεν προέρχονται μονό από το εξωτερικό περιβάλλον μιας εταιρίας, αλλά πολλές φόρες κι από τους ίδιους τους υπαλλήλους. Έτσι τα συστήματα αυτά ελέγχουν μονό έναν υπολογιστή, στον οποίο έχει τοποθετηθεί κατάλληλο λογισμικό που παρακολουθεί συγκεκριμένα αρχεία καταγραφής. Σε περίπτωση που παρατηρηθεί αλλοίωση, θεωρείται πως έχει υπεισέρθει κακόβουλη δραστηριότητα.

Η κατηγορία αυτή θεωρείται ως υποκατηγορία των Συστημάτων Ανίχνευσης Επιθέσεων που συλλέγουν πληροφορίες από υπολογιστές και δεν χρησιμοποιείται τόσο συχνά όσο οι δυο προηγούμενες κατηγορίες. Χρησιμοποιούνται αρχεία καταγραφής των εφαρμογών για να εντοπιστούν πιθανές επιθέσεις, οι οποίες επιχειρούνται στο επίπεδο της εφαρμογής.

3.3.1.1 ΤΑ ΑΝΤΑΝΑΚΛΑΣΤΙΚΑ ΤΩΝ ΣΑΕ
Από τη στιγμή που θα εντοπιστεί η επίθεση στο σύστημα, αναιρεί μια σειρά από εντολές ,συμφωνά με τις ρυθμίσεις που του έχουν γίνει, για την αντιμετώπισή της. Οι αντιδράσεις των ΣΑΕ διακρίνονται στις ενεργητικές και στις παθητικές.

Ενεργητικές αντιδράσεις: Στην κατηγορία των ενεργητικών αντιδράσεων το σύστημα από τη στιγμή που θα εντοπίσει μια επίθεση θα ξεκινήσει μια σειρά ενεργειών για την παρεμπόδισή της.

Όταν το σύστημα δεν είναι σίγουρο για το μέγεθος της ζημιάς που μπορεί να προκαλέσει η επίθεση, τότε δεν αντιδρά αλλά περιμένει να συγκεντρώσει περισσότερες πληροφορίες για να επαναξιολογήσει την κατάσταση. Όταν αυτό γίνει, τότε θα ενεργοποιήσει το firewall για να εμποδίσει την εισβολή στο δίκτυο.

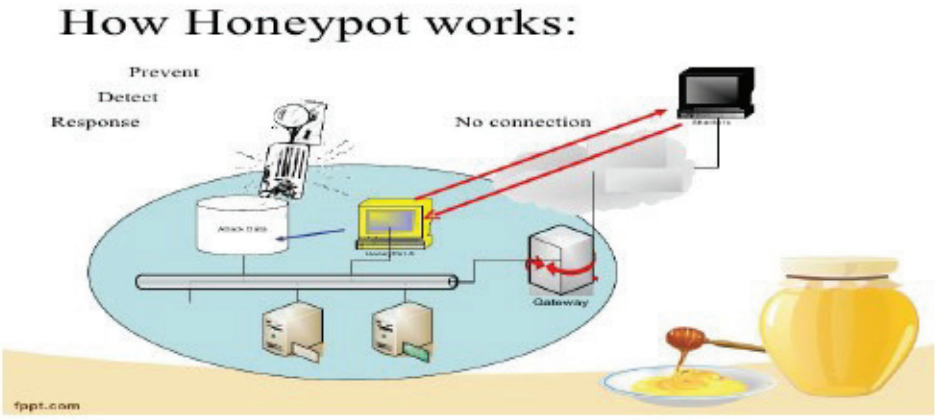
Παθητικές αντιδράσεις: Στις παθητικές αντιδράσεις το ΣΑΕ δεν ακολουθεί καμία ενέργεια. Στην περίπτωση που παρατηρηθεί εισβολή, αυτό που κάνει είναι να ενημερώσει τον διαχειριστή ή τον υπεύθυνο ασφάλειας για το πρόβλημα. Έπειτα γίνεται αξιολόγηση της κατάστασης της επίθεσης.
Τα μέσα και οι τρόποι ειδοποίησης του διαχειριστή εξαρτώνται άμεσα από τον παράγοντα αυτό.

3.3.1.2 ΚΑΤΗΓΟΡΙΕΣ ΣΑΕ

Στις ειδικές κατηγορίες ΣΑΕ εντάσσονται εργαλεία ανίχνευσης εισβολών που αποτελούν επιμέρους συστήματα και είναι εξαιρετικά απλά στη λειτουργία τους.
Αυτά είναι :
Τα συστήματα έλεγχου ακεραιότητας: Τα συστήματα αυτά παρακολουθούν κρίσιμα αρχεία, όπως τα αρχεία συστήματος, προκειμένου να εντοπίσουν τυχόν μεταβολές. Έχουν επίσης τη δυνατότητα να παρακολουθούν τους λογαριασμούς των χρηστών και να εντοπίζουν εάν κάποιος απλός χρήστης έχει αποκτήσει δικαιώματα διαχειριστή.

Συστήματα παρακολούθησης αρχείων καταγραφής: τα συστήματα αυτά δημιουργούν έναν φάκελο από αρχεία καταγραφής, τα οποία προέρχονται από τις υπηρεσίες του δικτυού. Στη συνέχεια παρακολουθούν τα αρχεία, καταγράφουν τις συνηθισμένες λειτουργίες του συστήματος και βασιζόμενα σε αυτές, προσπαθούν να εντοπίσουν πιθανές επιθέσεις.

Honeypots: πρόκειται για εικονικά συστήματα, τα οποία προσπαθούν να ξεγελάσουν τον επιτιθέμενο, δίνοντας του την εντύπωση ότι είναι πολύ εύκολο να εισβάλει στο σύστημα. Όταν λοιπόν πραγματοποιηθεί η εισβολή το σύστημα θα έχει καταγράψει όλες τις μεθόδους και τις τεχνικές που χρησιμοποίησε ο επιτιθέμενος



3.3.2 ΕΛΕΓΧΟΣ ΣΥΣΤΗΜΑΤΩΝ

Με τον έλεγχο των αρχείων καταγραφής του συστήματος μπορεί να εντοπιστεί μια επίθεση. Σε κάθε λειτουργικό σύστημα υπάρχουν εργαλεία ελέγχου. Στις επαγγελματικές εκδόσεις των πρόσφατων λειτουργικών συστημάτων της Microsoft, υπάρχουν τρία βασικά χαρακτηριστικά:

Application log, τα οποία περιέχουν μηνύματα, πληροφορίες κατάστασης και άλλα γεγονότα πουαναφέρονται από μη ζωτικές υπηρεσίες των Windows.

System log, στα οποία καταγράφονται σφάλματα αρχείων, προειδοποιήσεις και γεγονότα, τα οποία δημιουργούνται από το ίδιο το λειτουργικό σύστημα και σχετίζονται με υπηρεσίες του συστήματος.

Security log, στο οποίο καταγράφονται αρχεία που σχετίζονται με την πολιτική ελέγχου που έχει καθοριστεί από το διαχειριστή του λειτουργικού συστήματος.

3.4 ΑΝΤΙΜΕΤΩΠΙΣΗ ΚΑΤΑΣΤΡΟΦΩΝ

Η πρόληψη της επίθεσης και η αντιμετώπιση της απειλής, από τη στιγμή που αυτή θα εντοπιστεί, είναι δυο βασικά στάδια με τα οποία μπορούμε να προλάβουμε τις σοβαρότερες ζημιές στο υπολογιστικό σύστημα. Υπάρχουν όμως και περιπτώσεις

κατά τις οποίες το στάδιο της πρόληψης και της αντιμετώπισης μιας επίθεσης δεν αρκούν για να εμποδίσουν τον εισβολέα. Όταν ο εισβολέας καταφέρει να εισχωρήσει στο υπολογιστικό σύστημα τότε ξεκινάει και ο υπολογισμός της ζημιάς. Σε αυτό το σημείο έρχεται και η διαδικασία της αντιμετώπισης των καταστροφών.

Είναι απαραίτητο να αποθηκεύονται τα στοιχειά ενός υπολογιστή σε μονάδες αποθήκευσης (πχ cdR) προκειμένου να μην χαθούν μετά από μια ενδεχόμενη καταστροφή του υπολογιστή. Αυτή είναι επιτακτική ανάγκη για τους οργανισμούς που στα συστήματα τους περιέχουν υλικό αρκετά σημαντικό και ζωτικής σημασίας. Καλό θα ήταν να υπάρχουν εφεδρικά αρχεία που θα βοηθήσουν στη γρηγορότερη και λιγότερο ζημιογόνα αντιμετώπιση της καταστροφής. Θα πρέπει παρόλα αυτά να λάβουμε υπόψη μας πως επίθεση δεν είναι μόνο ο επιτιθέμενος, αλλά και τα φυσικά αίτια, όπως είναι το ξέσπασμα πυρκαγιάς, ο σεισμός, η πλημμύρες, η φυσική κλοπή. Η απώλεια δεδομένων ενός οργανισμού μπορεί να έχει απρόβλεπτες συνέπειες και να οδηγήσουν σε ολοκληρωτική οικονομική καταστροφή.

Για τη λήψη εφεδρικών αντιγράφων χρησιμοποιούνται μια σειρά από τεχνικές:
Το σύστημα ανάνηψης από καταστροφές αποτελεί αναπόσπαστο κομμάτι κάθε οργανισμού που θέλει να διαφυλάξει τα δεδομένα του. Ένα τέτοιο σύστημα αποτελείται από επιμέρους υποσυστήματα τα οποία διασφαλίζουν την ακεραιότητα των δεδομένων από κάθε είδους καταστροφή ή απειλή. Ωστόσο, οι λειτουργίες αυτές εξαρτώνται από: το είδος των δεδομένων που θα αποθηκευτούν:

- το είδος των δεδομένων που θα αποθηκευτούν εξαρτάται από τις ανάγκες που πρέπει να καλυφτούν αλλά και από το χρηματικό πόσο που μπορεί να διατεθεί. Έτσι, μικρές επιχειρήσεις αποθηκεύουν μόνο τα ζωτικής σημασίας αρχεία σε αντίθεση με τους μεγάλους οργανισμούς που αποθηκεύουν και τα περαιτέρω δεδομένα.
- τη συχνότητα της αποθήκευσης: η συχνότητα της αποθήκευσης των δεδομένων αναφέρεται σε παράγοντες όπως είναι ο ρυθμός με τον όποιο αλλάζουν τα δεδομένα, η ποσότητα των δεδομένων για την οποία απαιτείται λήψη εφεδρικών αντιγράφων, το χρονικό διάστημα στο όποιο μπορεί να λειτουργήσει ο οργανισμός χωρίς δεδομένα και το μέσο στο όποιο θα γίνει η αποθήκευση των εφεδρικών αντιγράφων.
- το σημείο που θα αποθηκευτούν τα αρχεία: η αποθήκευση των δεδομένων μπορεί να γίνει σε μαγνητικά μέσα, καθώς και σε άλλους τοπικούς ή απομακρυσμένους δίσκους. Η αποθήκευση αφορά την ασφάλεια αυτών των μέσων και τη δυνατότητά τους να διατηρούν τα αρχεία σε άριστη κατάσταση. Σε περίπτωση που υπάρχει οικονομική ευχέρεια τότε καλό θα είναι να τοποθετούνται εφεδρικοί υπολογιστές στους οποίους θα γίνεται πλήρη αποθήκευση των δεδομένων των βασικών υπολογιστών.

Η λήψη εφεδρικών αντιγράφων είναι ένα μέρος του συστήματος ανάνηψης

καταστροφών. Ακόμα κι όταν το κεφάλαιο μιας επιχείρησης ή ενός οργανισμού δεν αρκεί για την προμήθεια ενός συστήματος ανάνηψης καταστροφών, θα πρέπει να εξασφαλίσει τα δεδομένα με τη λήψη εφεδρικών αντιγράφων, η οποία μπορεί να ολοκληρωθεί με τη χρήση διαφόρων εφαρμογών που κυκλοφορούν στο εμπόριο για το σκοπό αυτό. Σε μια τέτοια εφαρμογή μεταφέρονται όλα τα αρχεία που βρίσκονται στον σκληρό δίσκο του υπολογιστή. Έτσι όταν ο σκληρός δίσκος υποστεί βλάβη γίνεται πλήρης αποκατάσταση και ο νέος δίσκος περιέχει ακριβώς τα δεδομένα με του παλιού δίσκου.

Τη διαδικασία της λήψης εφεδρικών αντιγράφων τη διακρίνουμε σε τρεις κατηγορίες:
i) Στην πλήρη λήψη αντιγράφων που λαμβάνονται εφεδρικά αντίγραφα από όλα τα αρχεία του συστήματος,
ii) στην λήψη τροποποιημένων αντιγράφων όπου λαμβάνονται αντίγραφα μόνο από τα αρχεία και
iii) στη λήψη διαφοροποιημένων αντιγράφων των αρχείων που έχουν διαφοροποιηθεί από την τελευταία πλήρη λήψη.

3.5 ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ ΚΑΙ ΑΣΦΑΛΕΙΑ

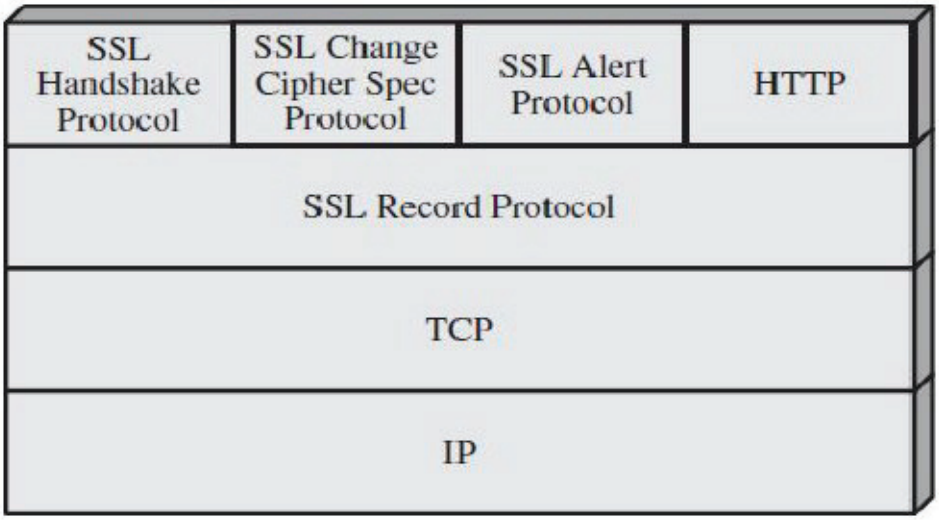
Το ηλεκτρονικό ταχυδρομείο χρησιμοποιείται ευρέως σήμερα, λόγο της ταχύτητας, της δυνατότητας μαζικής αποστολής μηνυμάτων αλλά κι επειδή είναι ανέξοδο. Αυτό που απασχολείτον χρήστη είναι η εμπιστευτικότητα, η ακεραιότητα και η αυθεντικότητα του μηνύματος. Λόγω της διαδεδομένης χρήσης του, το ηλεκτρονικό ταχυδρομείο αποτελεί συνήθως το στόχο για την μόλυνση και τη μετάδοση των ιών. Αυτό καθιστά επιτακτική την ανάγκη εγκατάστασης λογισμικού antivirus και της συνεχούς ενημέρωσής του. Οι ιοί μεταδίδονται με μηνύματα που συνήθως έχουν έναν άγνωστο αποστολέα για αυτό και χρησιμοποιούν τίτλους – θέματα που κινούν την περιέργεια στον παραλήπτη και που θα τον «πείσουν» να τα ανοίξει και εν συνεχεία να μολυνθεί.

Εκτός από τους ιούς υπάρχει και το spamming, η μαζική αποστολή μηνυμάτων με διαφημιστικό κυρίως περιεχόμενο αλλά μερικές φορές παραπλανητικό. Υπάρχουν πλέον στο εμπόριο λογισμικά που αποτρέπουν το spamming και χρησιμοποιούνται όταν το πρόβλημα παρατηρείται σε μεγάλο βαθμό και καταλήγει ενοχλητικό.
Θα πρέπει να δίνεται μεγάλη προσοχή και βαρύτητα στην αποστολή των μηνυμάτων μέσω του ηλεκτρονικού ταχυδρομείου. Όπως ήδη έχει γίνει λόγος, είναι πολύ εύκολο να παραβιαστούν οι κωδικοί και να κοινοποιηθεί το περιεχόμενο σε κάποιο τρίτο πρόσωπο, αυτό σημαίνει ότι δεν θα πρέπει να αποστέλλονται κωδικοί αριθμοί ή αριθμοί pin τραπεζών μέσω του ηλεκτρονικού ταχυδρομείου και γενικότερα να μην διακινούνται πληροφορίες με ευαίσθητα προσωπικά δεδομένα. Η ασφάλεια που μπορούμε να έχουμε σε αυτή τη περίπτωση είναι η τακτική αλλαγή των κωδικών πρόσβασης. Ένας ασφαλής τρόπος επικοινωνίας είναι η χρήση κρυπτογράφησης με το πρωτόκολλο SSL.

3.6 ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΝΑΛΛΑΓΩΝ

Το ηλεκτρικό εμπόριο στις μέρες μας γνωρίζει μεγάλη επιτυχία αφού τώρα πια όλες οι αγορές μπορούν να γίνουν μπροστά από την οθόνη ενός υπολογιστή και η παραγγελία μπορεί να γίνει με το πάτημα ενός πλήκτρου. Αντίστοιχα έχουν διαμορφωθεί και τρόποι πληρωμής που είναι οι πιστωτικές ή χρεωστικές κάρτες. Φυσικά ούτε από αυτή τη διαδικασία θα μπορούσε να απουσιάζει η απάτη. Συνεπώς χρειάζεται πολύ μεγάλη προσοχή στις πηγές που απευθυνόμαστε και στις οποίες στη συνέχεια δίνουμε τον αριθμό των πιστωτικών καρτών. Όσο αφορά στον τρόπο ανταλλαγής των πληροφοριών θα πρέπει να παρέχονται πιο ασφαλείς δίαυλοι επικοινωνίας για τις συναλλαγές. Ως εκ τούτου δημιουργήθηκε μια σειρά από πρωτόκολλα επικοινωνίας, τα οποία στοχεύουν στην προστασία δεδομένων.
Από τα πιο σημαντικά πρωτόκολλα είναι το SSL και το SET.

Πρωτόκολλο SSL

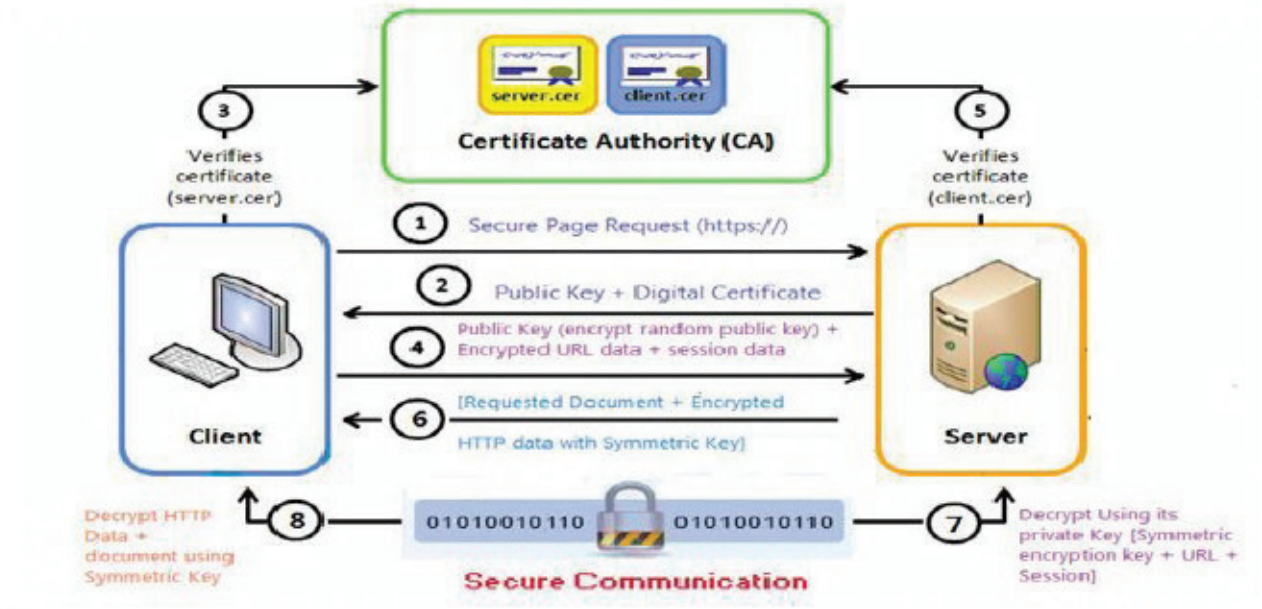


Το πρωτόκολλο SSL αναπτύχθηκε από την Netscape Communications Corporation για την ασφαλή επικοινωνία ευαίσθητων πληροφοριών όπως προσωπικά στοιχεία και αριθμούς πιστωτικών καρτών. Η πρώτη σχεδίαση του πρωτοκόλλου έγινε τον Ιούλιο του 1994 και αποτελούσε την πρώτη έκδοση (version 1.0) και τον Οκτώβριο του ίδιου χρόνου δημοσιοποιήθηκε υπό την μορφή RFC (Request For Comments). Τον Δεκέμβριο του 1994 εκδίδεται μια επαναθεώρηση του πρωτοκόλλου, η δεύτερη έκδοση του (version 2.0). Η παρούσα έκδοση του SSL, version 3.0, παρουσιάσθηκε στο κοινό στα τέλη του 1995, ενώ από τα μέσα του 1995 είχε αρχίσει να εφαρμόζεται σε προϊόντα της εταιρίας, όπως τον Netscape Navigator.

Επειδή η Netscape επιθυμούσε την παγκόσμια υιοθέτηση του πρωτοκόλλου γεγονός που ερχόταν σε σύγκρουση με τους νόμους των Ηνωμένων Πολιτειών περί εξαγωγή κρυπτογραφικών αλγορίθμων, αναγκάστηκε να επιτρέψει την χρήση ασθενών αλγορίθμων στις εξαγόμενες εφαρμογές. Πιο συγκεκριμένα, δημιούργησε παραλλαγές των αλγόριθμων RC4-128 και RC2-128 που στην πραγματικότητα χρησιμοποιούν κλειδιά των 40 bits.

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί σαν client και το άλλο σαν server. Η εξασφάλιση του απορρήτου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol. Παρέχει, επιπλέον, υποχρεωτική πιστοποίηση της ταυτότητας του server και προαιρετικά της ταυτότητας του client, μέσω έγκυρων πιστοποιητικών από έμπιστες Αρχές Έκδοσης Πιστοποιητικών (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων, εφαρμόζοντας την τεχνική των Message Authentication Codes (MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την

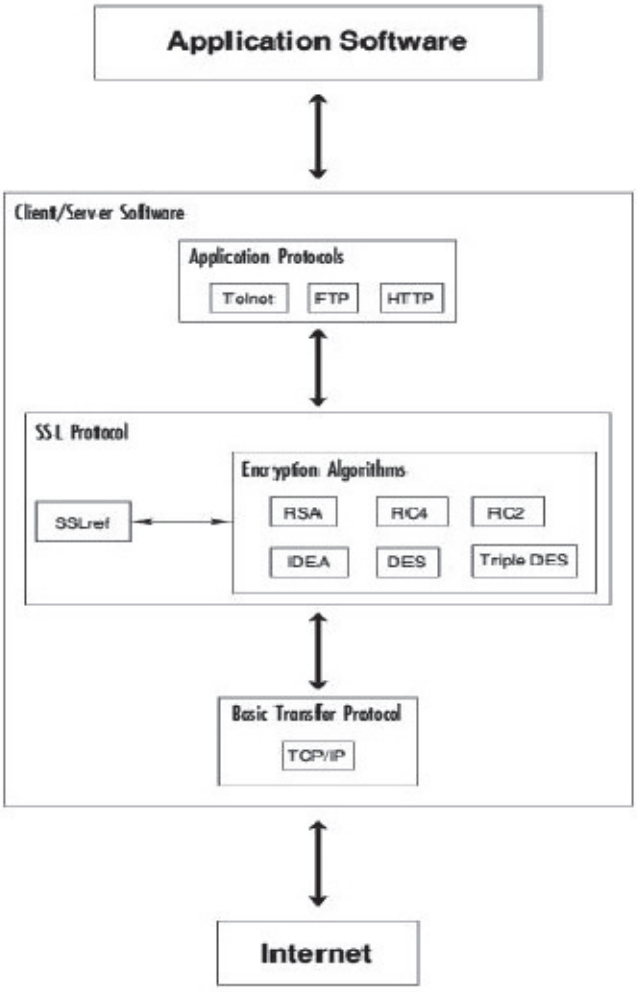
πληροφορία χωρίς να γίνει αντιληπτός. Όλα τα παραπάνω γίνονται με τρόπο διαφανές και απλό.

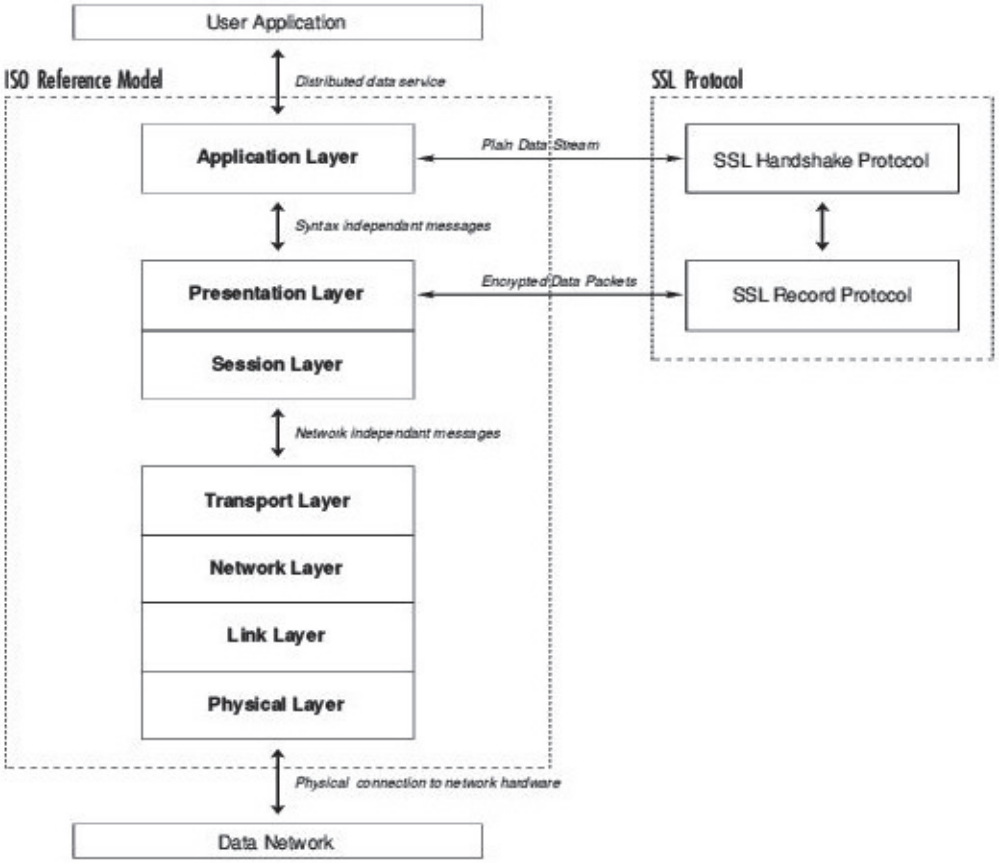


Η έκδοση 3 του πρωτοκόλλου κάλυψε πολλές αδυναμίες της δεύτερης. Οι σημαντικότερες αλλαγές έχουν να με την μείωση των απαραίτητων μηνυμάτων κατά το handshake για την εγκαθίδρυση της σύνδεσης, την επιλογή των αλγόριθμων συμπίεσης και κρυπτογράφησης από τον server και την εκ νέου διαπραγμάτευση του master-key και session-id. Ακόμα αυξάνονται οι διαθέσιμοι αλγόριθμοι και προστίθενται νέες τεχνικές για την διαχείριση των κλειδιών.

Συμπερασματικά μπορούμε να πούμε πως η έκδοση 3 του SSL είναι πιο ολοκληρωμένη σχεδιαστικά, με μεγαλύτερο εύρος υποστήριξης εφαρμογών και λιγότερες ατέλειες. Παρ' όλο που είναι συμβατή με την δεύτερη έκδοση, η χρήση της τελευταίας δεν πρέπει να προτιμάται.

Το SSL μπορεί να τοποθετηθεί στην κορυφή οποιουδήποτε πρωτοκόλλου μεταφοράς, δεν εξαρτάται από την ύπαρξη του TCP/IP και τρέχει κάτω από πρωτόκολλα εφαρμογών όπως το HTTP, FTP καιTELNET. Μια αναπαράσταση του πρωτοκόλλου SSL βλέπουμε παρακάτω


Application Software
Client/Server Software
Application Protocols
Telnet
FTP
HTTP
SSL Protocol
SSLref
Encryption Algorithms
RSA
RC4
RC2
IDEA
DES
Triple DES
Basic Transfer Protocol
TCP/IP
Internet



Είναι σημαντικό κάθε νέο πρωτόκολλο επικοινωνίας να συμμορφώνεται με το OSI μοντέλο, έτσι ώστε να μπορεί εύκολα να αντικαταστήσει κάποιο υπάρχον πρωτόκολλο ή να ενσωματωθεί στην υπάρχουσα δομή πρωτοκόλλων.

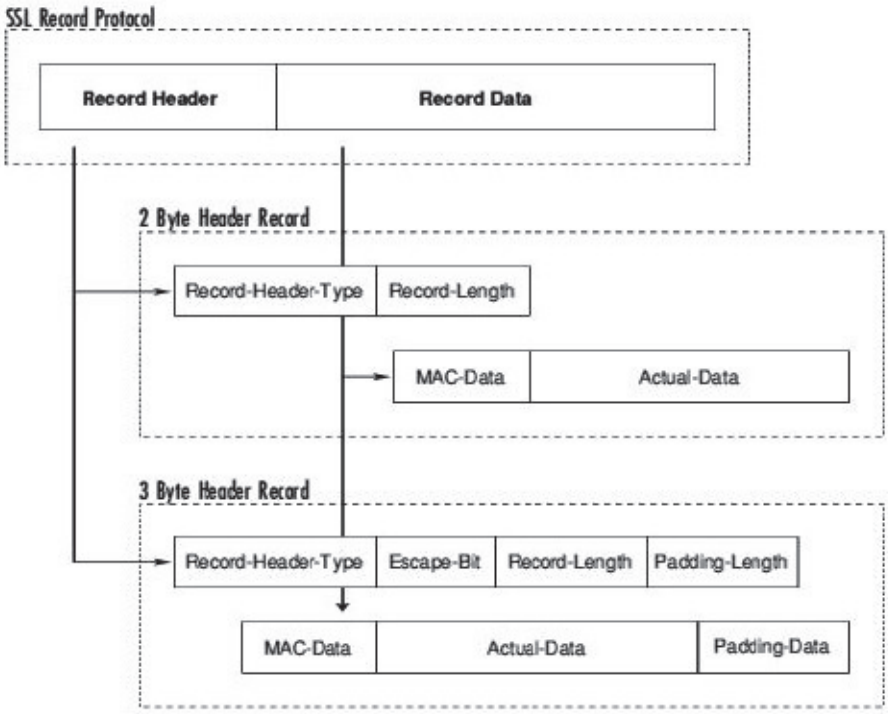
Το SSL χωρίζεται σε δύο μέρη, το SSL Handshake Protocol (SSLHP) και το SSL Record Protocol (SSLRP). Το SSLHP διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του server και εάν ζητηθεί και του client. Το SSLRP συλλέγει τα δεδομένα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

Βλέπουμε πως το SSL λειτουργεί επιπρόσθετα της υπάρχουσας δομής του OSI και όχι σαν πρωτόκολλο αντικατάστασης. Επίσης είναι πασιφανές ότι η χρήση του SSL δεν αποκλείει την χρήσης άλλου μηχανισμού ασφαλείας που λειτουργεί σε υψηλότερο επίπεδο, για παράδειγμα το S/HTTP που εφαρμόζεται στο επίπεδο Εφαρμογών, πάνω από το SSL.

Λειτουργία του SSL

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 συμπληρωματική 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 χρησιμοποιηθεί η επικεφαλίδα των 2 bytes.

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).

Αντοχή του SSL σε Γνωστές Επιθέσεις

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.

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.

Brute Force Attack

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.

Replay Attack

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 επίθεσηreplay 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.

Man-In-The-Middle-Attack

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.

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.

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 TELNETεφαρμογής), 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.

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.

Πρωτόκολλο SET

Το SET (Secure Electronic Transaction) είναι ένα πρωτόκολλο εμπορικών συναλλαγών με τη χρήση καρτών σε ανοικτά δίκτυα, το οποίο αναπτύχθηκε από την MasterCard και την Visa σαν μια μέθοδος εξασφάλισης των συναλλαγών με τη χρήση καρτών διαμέσου του Internet.

Η διαδικασία περιλαμβάνει ένα αριθμό ελέγχων ασφαλείας που πραγματοποιείται με τη χρήση ψηφιακών πιστοποιητικών που χορηγούνται στους εμπλεκόμενους αγοραστές, εμπόρους και τράπεζες.

Προδιαγραφές

Το SET έχει δημιουργηθεί βάση συγκεκριμένων προδιαγραφών που προήλθαν από τις απαιτήσεις των επιχειρήσεων και αφορούσαν τις συναλλαγές τους. Αυτές οι προδιαγραφές είναι:

1. Παροχή προστασίας των οικονομικών δεδομένων ή και άλλων που διακινούνται μαζί τους από υποκλοπή
2. Διασφάλιση της ακεραιότητας των δεδομένων.
3. Παροχή διαδικασιών πιστοποίησης ταυτότητας του κατόχου κάρτας.
4. Παροχή υπηρεσιών πιστοποίησης των εμπόρων που μπορούν να δεχθούν την πληρωμή με τη χρήση τέτοιας μεθόδου, που προκύπτει από τη σχέση τους με κάποιο οικονομικό ίδρυμα παροχής καρτών.
   Διασφάλιση της χρήσης των καλύτερων τεχνικών ασφάλειας και σχεδίασης συστημάτων για την προστασία όλων των νόμιμα εμπλεκομένων πλευρών.
5. Η δημιουργία ενός πρωτοκόλλου το οποίο να είναι ανεξάρτητο από τους μηχανισμούς ασφάλειας του επιπέδου μεταφοράς χωρίς όμως και να αποτρέπει τη χρήση τους.
6. Να είναι διαλειτουργικό (όλοι οι κύριοι browsers δουλεύουν με όλους τους κύριους servers και οι τελευταίοι με τη σειρά τους δεν θα έχουν πρόβλημα συμβατότητας με τους Payment Gateway Servers).
7.

Συστατικά Στοιχεία του SET

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

1. 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).

2. 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 τουSET.

3. 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.

4. 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

ΚΕΦΑΛΑΙΟ 4

ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

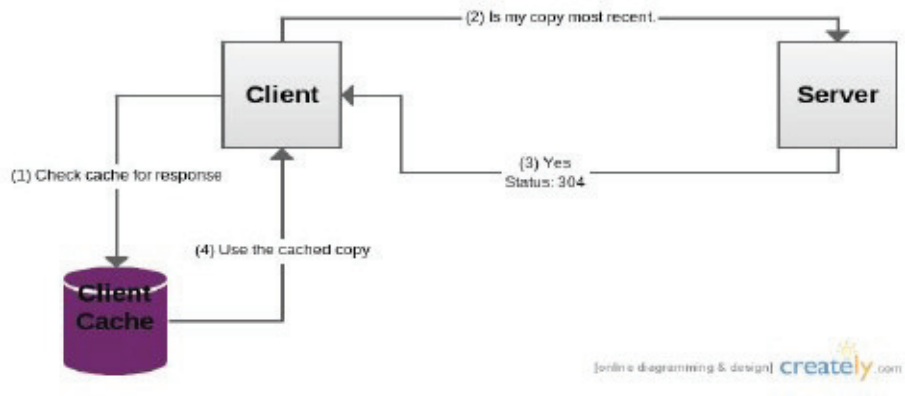
Για την αντιμετώπιση του συνόλου των κίνδυνων ασφάλειας, κάθε οργανισμός εφαρμόζει μια πολιτική ασφάλειας που έχει θέσει η διοίκηση του οργανισμού. Η πολιτική ασφάλειας είναι το γραπτό κείμενο το οποίο καθορίζει τους κανόνες που θα πρέπει να ακολουθούνται για την ασφάλεια του πληροφοριακού συστήματος του οργανισμού από υφιστάμενους πληροφοριακούς κινδύνους. Για τη σύνταξη του κειμένου της πολιτικής ασφαλείας ακολουθούνται δυο στάδια.
Στο πρώτο στάδιο, πριν τη σύνταξη του κειμένου, προσδιορίζονται οι κίνδυνοι ασφαλείας που διατρέχει ο οργανισμός. Πραγματοποιείται μια ποσοτική ανάλυση του κίνδυνου. Συγκεκριμένα καθορίζεται: α) το είδος των κίνδυνων ασφαλείας έναντι των οποίων είναι ευάλωτος ο οργανισμός, β) η πιθανότητα να προκύψει ο κίνδυνος και γ) το κόστος που θα έχει ο οργανισμός σε περίπτωση που αυτός πραγματοποιηθεί.
Εκτός από την ποσοτική ανάλυση χρησιμοποιείται και η ποιοτική ανάλυση. Στην ποιοτική ανάλυση δεν έχουμε την λογική των πιθανοτήτων αλλά λαμβάνονται υπόψη άλλοι παράγοντες όπως οι πιθανές απειλές και τα χαρακτηριστικά του συστήματος που το καθιστούν ευάλωτο μπροστά στις απειλές αυτές.
Στο δεύτερο στάδιο γίνεται η σύνταξη του κειμένου της πολιτικής ασφάλειας το όποιο θα πρέπει να χωριστεί σε δυο βασικά έγγραφα. Το πρώτο θα περιγράφει τις γενικές πολιτικές και το δεύτερο θα περιγράφει συγκεκριμένες διαδικασίες. Αυτό το στάδιο θα πρέπει να τελεστεί από άνθρωπο με γνώση κι εμπειρία. Σημαντικό είναι οι κανόνες να είναι γραμμένοι σε απλή και κατανοητή για όλους γλώσσα.

4.1 PHISING ΚΑΙ ΑΣΦΑΛΕΙΑ

“ 

Η χρήση τεχνολογικών μέσων για την προστασία από επιθέσεις Phishing αφορά σε τεχνολογίες ασφαλείας πληροφοριακών συστημάτων και ενδείκνυται να γίνεται σε τουλάχιστον τρία επίπεδα προστασίας:
1. client-side επίπεδο
2. server-side επίπεδο
3. services-provider-side επίπεδο

CLIENT-SIDE ΕΠΙΠΕΔΟ



Το επίπεδο client-side αφορά στην αντιμετώπιση του προβλήματος του Phishing από τους τελικούς χρήστες—καταναλωτές (end-users). Στο επίπεδο αυτό μπορεί να γίνει τεχνολογιών ασφαλείας πληροφοριακών συστημάτων:
1. χρησιμοποίηση desktop protection agents

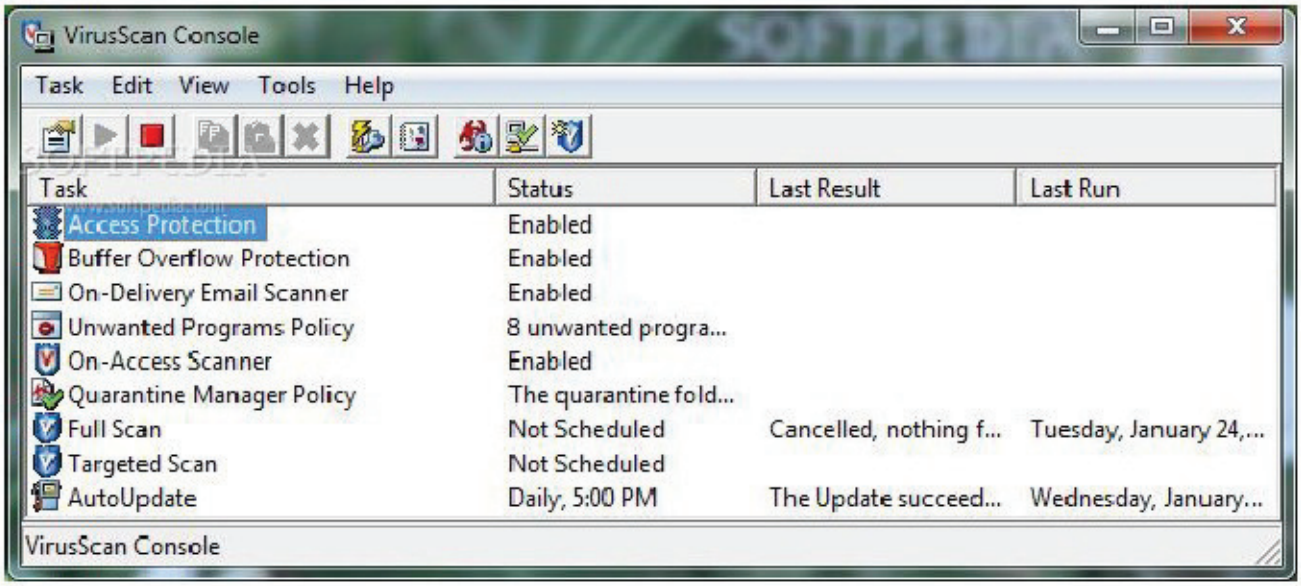
2. κατάλληλη διαρρύθμιση των παραμέτρων επικοινωνίας

3. απενεργοποίηση των παραμέτρων του λογισμικού προγράμματος φυλλομέτρησης ιστοσελίδων

4. χρησιμοποίηση ψηφιακής υπογραφής και πιστοποίησης ηλεκτρονικής αλληλογραφίας

5. εγρήγορση σε ζητήματα ασφαλείας

Η χρησιμοποίηση των desktop protection agents μπορεί να περιλαμβάνει:
1. anti-virus προστασία
2. προσωπικό firewall
3. σύστημα αναγνώρισης ενεργειών παραβίασης της ασφάλειας του συστήματος (intrusion detection system προστασία)
4. προστασία από την απρόσκλητη εμπορική επικοινωνία (anti-spam προστασία)
5. προστασία από κακόβουλα, κυρίως κατασκοπευτικά, λογισμικά προγράμματα (malware και spyware προστασία)



Η χρησιμοποίηση των κατάλληλα συνδυασμένων desktop protection agents αποσκοπεί στην παροχή προστασίας του πληροφοριακού συστήματος του τελικού χρήστη—καταναλωτή με την ενεργοποίηση των εξής λειτουργιών:
1. ανίχνευση και μπλοκάρισμα σε πραγματικό χρόνο («on the fly») κάθε απόπειρας διάρρηξης πληροφοριακού συστήματος, εισαγωγής και εγκατάστασης σ' αυτό ζημιογόνου λογισμικού κώδικα υποκρυπτόμενου σε συνημμένα αρχεία ηλεκτρονικών μηνυμάτων, εκτελέσιμα αρχεία, μεταφερόμενα αρχεία, DHTML, ή οποιοδήποτε άλλο περιεχόμενο.
2. ανίχνευση και μπλοκάρισμα σε πραγματικό χρόνο της απρόσκλητης εμπορικής επικοινωνίας.
3. διαρκώς ανανεώσιμη anti-virus και anti-spam προστασία με αυτοματοποιημένη μεταφορά και εγκατάσταση κάθε νέας έκδοσης u964 των εν λόγω τεχνολογιών ασφαλείας

4. ανίχνευση και μπλοκάρισμα σε πραγματικό χρόνο κάθε μη εξουσιοδοτημένης απόπειραςωσύνδεσης και επικοινωνίας που επιχειρεί το πληροφοριακό σύστημα του τελικού χρήστη—καταναλωτή με οποιοδήποτε τρίτον (unauthorized outbound connections) συνεπεία λειτουργίας εκτελέσιμου λογισμικού κώδικα ή οποιασδήποτε εφαρμογής που ενεργούν από το πληροφοριακό σύστημα του τελικού

χρήστη-καταναλωτή.
5. ανίχνευση ανωμαλιών σε οποιαδήποτε εισερχόμενη ή εξερχόμενη επικοινωνία προς και από το δίκτυο πληροφοριακών συστημάτων του τελικού χρήστη-καταναλωτή.
6. ανίχνευση κάθε εισαγωγής και εγκατάστασης spyware και malware λογισμικού και μπλοκάρισμα κάθε εξερχόμενης επικοινωνίας από το πληροφοριακό σύστημα του τελικού χρήστη- καταναλωτή προς διαδικτυακούς τόπους που παρακολουθούν ή με οποιονδήποτε τρόπο συνδράμουν την κυκλοφορία spyware και malware.
Η κατάλληλη διαρρύθμιση των παραμέτρων επικοινωνίας υπαγορεύει την αποφυγή εξαιρετικά πολύπλοκων λογισμικών προγραμμάτων και εφαρμογών που να είναι σε λειτουργία από το πληροφοριακό σύστημα του τελικού χρήστη-καταναλωτή. Τα περισσότερα από τα πιο εμπορικά λογισμικά προϊόντα επιτρέπουν πλέον την απενεργοποίηση από τον χρήστη-καταναλωτή λειτουργιών του προϊόντος που διατίθενται ως προεπιλεγμένες λειτουργίες (default settings). Ο τελικός χρήστης-καταναλωτής μπορεί, επίσης, να απενεργοποιήσει τις παραμέτρους του browser που είναι ευάλωτες, ή τουλάχιστον οι πιο συνήθης στην προτίμηση και κακόβουλη χρήση τους από τους Phishers για την οργάνωση και εκτέλεση επίθεσης Phishing42. Παράμετροι του browser που μπορούν να απενεργοποιηθούν περιλαμβάνουν:
1. η λειτουργία window popup
2. η υποστήριξη Java runtime
3. η υποστήριξη ActiveX λειτουργίας
4. η αυτοματοποιημένη εκτέλεση πολυμεσικών εφαρμογών (multimedia autoplay και auto-execute extensions)
5. η αποθήκευση μη ασφαλών (non-secure) cookies

SERVER-SIDE ΕΠΙΠΕΔΟ

Το επίπεδο server-side αφορά στην αντιμετώπιση του προβλήματος του Phishing από τα εκτεθειμένα σε ενδεχόμενη επίθεση Phishing πληροφοριακά συστήματα μίας επιχείρησης ή ενός οργανισμού. Οι προτεινόμενες λύσεις για την αντιμετώπιση του προβλήματος στο επίπεδο αυτόπεριλαμβάνουν:
1. διαρκή εγρήγορση των συνδεόμενων με το πληροφοριακό σύστημα καταναλωτών αναφορικά με ζητήματα ασφαλείας
2. πιστοποίηση προέλευσης πληροφοριών.
3. χρησιμοποίηση token-based συστημάτων πιστοποίησης

Η διαρκής εγρήγορση σε ζητήματα ασφαλείας μπορεί να περιλαμβάνει:
1. διαρκή υπενθύμιση της φύσης του προβλήματος και της τυπολογίας των επιθέσεων.
2. εξασφάλιση στους συνδεόμενους με το πληροφοριακό σύστημα καταναλωτές μίας μεθόδου εύκολης και γρήγορης αναφοράς επιθέσεων Phishing.
3. παροχή οδηγιών στους συνδεόμενους με το πληροφοριακό σύστημα καταναλωτές σχετικών με την επαλήθευση της γνησιότητας του περιεχομένου ενός διαδικτυακού

τόπου ενός οργανισμού.
4. δημιουργία σαφούς και πλήρους πλαισίου κανόνων επικοινωνιακής πολιτικής ενός οργανισμού και χρήση αυτού.
5. άμεση ανταπόκριση και λήψη μέτρων αντιμετώπισης επιθέσεων Phishing που έχουν αναφερθεί δια της διαμορφωμένης και επιλεγμένης μεθόδου αναφοράς αυτών.

SERVICES PROVIDER-SIDE ΕΠΙΠΕΔΟ
Στο επίπεδο services provider-side αντιμετωπίζεται το πρόβλημα του Phishing από πάροχους υπηρεσιών. Οι προτεινόμενες λύσεις για την αντιμετώπιση του προβλήματος στο επίπεδο αυτό περιλαμβάνουν:
1. αυτοματοποιημένη πιστοποίηση των email server διευθύνσεων
2. ψηφιακή υπογραφή των emails
3. ανίχνευση του Διαδικτύου για ενδεχόμενη εκχώρηση σε τρίτον και χρήση από αυτόν των ονομάτων χώρου ενός οργανισμού
4. περιμετρική προστασία με gateway protection agents
5. ενεργή και διαρκής παρακολούθηση του Διαδικτύου

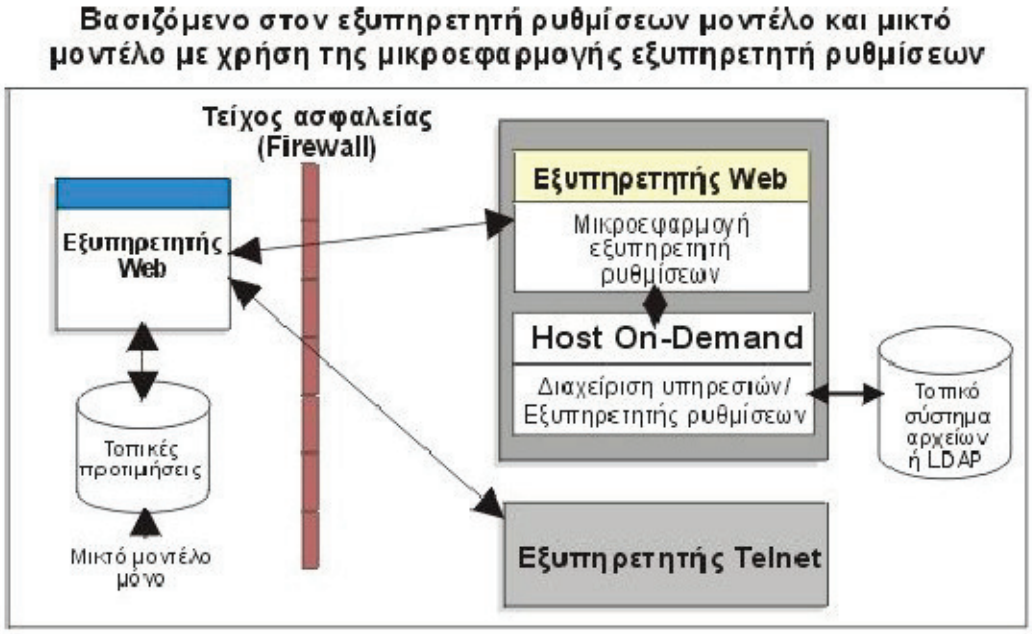
Η περιμετρική προστασία με gateway protection agents περιλαμβάνει:
1. gateway anti-virus σκανάρισμα
2. gateway anti-spam φιλτράρισμα
3. gateway φιλτράρισμα περιεχομένου
Η ενεργή και διαρκής παρακολούθηση του Διαδικτύου συνήθως πραγματοποιείται διαμέσου πάροχων υπηρεσιών οι οποίοι ενεργοποιούν agent-based bots για να παρακολουθούν το Διαδίκτυο και ανιχνεύουν στο περιεχόμενό του κάθε περίπτωση χρήσης του λογότυπου, σήματος, ή άλλου προστατευμένου νομικά περιεχόμενου ενός οργανισμού. Σε κάθε περίπτωση που τα agent-based bots διαπιστώνουν μη εξουσιοδοτημένη χρήση νομικά προστατευμένου περιεχόμενου ενός οργανισμού, λαμβάνονται μέτρα εναντίον του μη εξουσιοδοτημένου χρήστη”
(Παπαδόπουλος, 2005)

4.2 ΑΣΦΑΛΕΙΑ WEB ΕΞΥΠΗΡΕΤΩΝ ΚΑΙ WEB ΕΦΑΡΜΟΓΩΝ

Η ασφάλεια του εμπορίου στο διαδίκτυο είναι ίσως η μεγαλύτερη πρόκληση που έχουν να αντιμετωπίσουν οι “ειδικοί” στο χώρο του διαδικτύου. Η προστασία των ηλεκτρονικών συναλλαγών αποτελεί τη μια πτυχή του προβλήματος. Για να υπάρχει όμως ασφάλεια στις συναλλαγές απαιτείται η ύπαρξη ενός ασφαλούς εξυπηρετητή διαδικτύου (web server). Ο web εξυπηρετητής πρέπει να προστατεύει τα ευαίσθητα δεδομένα που στέλνονται από το πρόγραμμα πλοήγησης (web browser) του πελάτη στον εξυπηρετητή του καταστήματος. Οι web εξυπηρετητές διαχειρίζονται και διανέμουν τις πληροφορίες στο διαδίκτυο. Σήμερα οι web εξυπηρετητές αποτελούν τον αγαπημένο στόχο των hackers. Επιπλέον πολλές εφαρμογές διαδικτύου απαιτούν την αλληλεπίδραση του εξυπηρετητή διαδικτύου με βάσεις δεδομένων των εταιρειών, δημιουργώντας έτσι ένα σύνδεσμο με τα εσωτερικά τοπικά δίκτυα.
Επίσης το διαδίκτυο προσφέρει στις επιχειρήσεις αλλά και στους καταναλωτές μια

μοναδική ευκαιρία επικοινωνίας τόσο σε εθνικό όσο και σε παγκόσμιο επίπεδο. Το χαμηλό κόστος, η εύκολη πρόσβαση, η γρήγορη και συνεχής ενημέρωση, είναι μόνο μερικοί από τους παράγοντες που βοήθησαν στην ανάπτυξη του ηλεκτρονικού εμπορίου. Ωστόσο, από πολύ νωρίς φάνηκαν και τα προβλήματα τα οποία συνδέονται με το ηλεκτρονικό εμπόριο και τα οποία πρέπει να αντιμετωπιστούν αποτελεσματικά για την περαιτέρω εξέλιξη του. Ο πιο σημαντικός φραγμός για την υιοθέτηση του ηλεκτρονικού εμπορίου είναι η ασφάλεια των συναλλαγών. Για παράδειγμα, ο χρήστης που κάνει μια αγορά σε πραγματικό χρόνο (on-line) πρέπει να είναι σίγουρος ότι ο αριθμός της πιστωτικής του κάρτας δε θα υποκλαπεί. Κάθε φορά που συνδιαλέγεται δικτυακά με την τράπεζα του (e-banking) θέλει να γνωρίζει ότι όντως έρχεται σε επαφή με την ίδια την τράπεζα και όχι με κάποιον που επιχειρεί να τον εξαπατήσει. Όταν αποστέλλει στο διαδίκτυο ευαίσθητα δεδομένα, θέλει να ξέρει ότι δε θα έχει πρόσβαση σε αυτά κανείς άλλος εκτός από τον πραγματικό παραλήπτη τους. Μέσα σε αυτό το κλίμα, αυξάνονται δυστυχώς και οι ευκαιρίες για ηλεκτρονικές απάτες. Θύματα επιθέσεων, ενοχλητικών έως και επικίνδυνων “crackers”, πέφτουν συχνά ακόμη και μεγάλοι δικτυακοί τόποι όπως το Yahoo, το Amazon, το eBay. Η ασφάλεια web εφαρμογών γενικότερα και η ασφάλεια στο ηλεκτρονικό εμπόριο ειδικότερα, είναι ένας τεράστιος και σύνθετος στόχος. Πολλοί, ακούγοντας τον όρο ασφάλεια web εφαρμογών, έχουν την τάση να σκέφτονται αμέσως επιτιθέμενους που παραμορφώνουν ιστοσελίδες, κλέβουν αριθμούς πιστωτικών καρτών, και βομβαρδίζουν με μηνύματα ιστοσελίδες προκαλώντας επιθέσεις τύπου άρνησης υπηρεσίας (denial of service attack). Επίσης σκέφτονται τα προβλήματα που προκαλούν οι ιοί (viruses), οι δούρειοι ίπποι (Trojan horses) και τα σκουλήκια (worms).Αυτοί είναι οι τύποι προβλημάτων που απασχολούν περισσότερο το κοινό, λόγω του ότι αντιπροσωπεύουν μερικές από τις σημαντικότερες απειλές που αντιμετωπίζουν σήμερα οι web εφαρμογές. Τα παραπάνω, είναι μόνο μερικά από τα προβλήματα. Κάποια άλλα σημαντικά προβλήματα συχνά αγνοούνται. Οι εσωτερικές απειλές που τίθενται από απατεώνες διοικητές, από δυσαρεστημένους ή απρόσεκτους υπαλλήλους και από περιστασιακούς χρήστες θέτουν σημαντικό κίνδυνο.Όλες οι επιθέσεις σε επίπεδο εφαρμογών έχουν σαν στόχο να επωφεληθούν από τις υπάρχουσες αδυναμίες ασφάλειας με αποτέλεσμα να πλήξουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των επιχειρηματικών δεδομένων που επεξεργάζονται μέσω της εκάστοτε εφαρμογής. Οι συνέπειες από την παραβίαση της ασφάλειας είναι τεράστιες: απώλεια εισοδημάτων, ζημιά στην αξιοπιστία της επιχείρησης, νομική ευθύνη, και το χειρότερο για έναν οργανισμό ηλεκτρονικού εμπορίου είναι η απώλεια της εμπιστοσύνης του πελάτη.

4.2.1 Η έννοια των Web Εξυπηρετητών.



Οι web εξυπηρετητές είναι πολύπλοκα και εξειδικευμένα προγράμματα, τα οποία δίνουν τη δυνατότητα στις σελίδες HTML (Hypertext Markup Language) να καταστούν προσπελάσιμες από τα προγράμματα πλοήγησης, εφόσον υπάρχει σύνδεση του υπολογιστή με το διαδίκτυο. Είναι δηλαδή σχεδιασμένοι να δέχονται ανώνυμες αιτήσεις από άγνωστους υπολογιστές σε όλο το διαδίκτυο και να παραδίδουν τις ζητούμενες πληροφορίες γρήγορα και αποτελεσματικά. Δυστυχώς, όμως, δεν υπάρχει λογισμικό που η χρήση του να μην περικλείει κινδύνους και οι web εξυπηρετητές δεν αποτελούν εξαίρεση.
Πολλοί οργανισμοί χρησιμοποιούν web εξυπηρετητές, ο πηγαίος κώδικας των οποίων είναι ελεύθερα διαθέσιμος στο διαδίκτυο. Μονολότι αυτό επιτρέπει τη δοκιμή και τον έλεγχο του προγράμματος, δίνει τη δυνατότητα σε κάποιον, που έχει τις απαραίτητες γνώσεις, να ανακαλύψει ατέλειες που κάνουν τον web εξυπηρετητή ευάλωτο σε επιθέσεις. Ένας web εξυπηρετητής μπορεί να ενσωματώνει προγράμματα στις ηλεκτρονικές σελίδες του. Τα προγράμματα αυτά δημιουργούνται με το πρωτόκολλο Common Gateway Interface (CGI) και ονομάζονται CGI scripts. Τα CGI scripts, που εκτελούνται στην πλευρά του εξυπηρετητή κάθε φορά που κάποιος θέλει να συνδεθεί με αυτόν, μπορεί να είναι εξαιρετικά απλά, όπως για παράδειγμα ένας μετρητής που αυξάνει κάθε φορά που κάποιος επισκέπτεται τη σελίδα ή αρκετά πολύπλοκα, όπως για παράδειγμα αυτά που παρέχουν τη δυνατότητα για αγορά προϊόντων ή άλλες οικονομικές συναλλαγές μέσα από το διαδίκτυο.

4.2.2 Λειτουργίες των Web Εξυπηρετητών.

Οι web εξυπηρετητές εκτελούν τις παρακάτω λειτουργίες:
• Εξυπηρετούν αιτήσεις HTTP.

• Παρέχουν έλεγχο προσπέλασης, καθορίζοντας ποιος μπορεί να προσπελάσει συγκεκριμένους καταλόγους ή αρχεία στον εξυπηρετητή διαδικτύου.
• Εκτελούν scripts ή προγράμματα, είτε για να προσθέσουν λειτουργικότητα στις ιστοσελίδες, είτε για να παράσχουν πρόσβαση πραγματικού χρόνου (real - time access) σε βάσεις δεδομένων και σε άλλα δυναμικά δεδομένα.
• Καταγράφουν τις συναλλαγές ηλεκτρονικού εμπορίου που πραγματοποιούν οι χρήστες.
Οι εξυπηρετητές μπορούν να διακριθούν από τα εξής:

Πλατφόρμες: μερικοί είναι σχεδιασμένοι για συγκεκριμένη πλατφόρμα (π.χ. Windows), ενώ άλλοι για μια ποικιλία αυτών.
Απόδοση: αριθμός ταυτόχρονων αιτήσεων που μπορούν να χειριστούν, ταχύτητα επεξεργασίας, κλπ.
Ασφάλεια: δυνατότητα πρόσθετων υπηρεσιών ασφάλειας όπως υποστήριξη ανταλλαγής κρυπτογραφημένων δεδομένων
Εμπόριο: δυνατότητα προχωρημένων υπηρεσιών υποστήριξης ηλεκτρονικών συναλλαγών.

4.2.3 Σφάλματα στην Ασφάλεια του Web Εξυπηρετητή.

Τη διαμόρφωση του web εξυπηρετητή την αναλαμβάνει συνήθως κάποιος χρήστης/ διαχειριστής. Πρέπει να επισημανθεί ότι ένας εξυπηρετητής με κακή διαμόρφωση (configuration) μπορεί να δημιουργήσει προβλήματα ασφάλειας ακόμη και σε ένα πολύ καλά σχεδιασμένο σύστημα ασφάλειας. Για το λόγο αυτό, πρέπει να αναλαμβάνει τη διαχείριση του web εξυπηρετητή ένα έμπειρο και αξιόπιστο άτομο.
Ο εξυπηρετητής πρέπει να είναι και φυσικά ασφαλής. Αν ο web εξυπηρετητής βρίσκεται σε ένα εργαστήριο υπολογιστών, σε μια κοινή αίθουσα ή σε άλλες κοινές περιοχές, δεν είναι ασφαλής. Αν έχει το ρόλο ενός σταθμού εργασίας γενικού σκοπού, πιθανώς ούτε εκεί είναι ασφαλής. Ακόμη και αν το μηχάνημα απαιτεί ένα όνομα χρήστη και ένα κωδικό πρόσβασης, είναι απλό για κάποιον επιτιθέμενο να κλέψει ή να τροποποιήσει δεδομένα.
Η ικανότητα των web εξυπηρετητών να ενσωματώνουν CGI scripts περιπλέκει σημαντικά την εφαρμογή ενός συστήματος ασφάλειας. Τα CGI scripts προσθέτουν νέα χαρακτηριστικά και δυνατότητες σε έναν web εξυπηρετητή. Ταυτόχρονα όμως καθιστούν τον εξυπηρετητή πιο ευαίσθητο σε θέματα ασφάλειας. Για παράδειγμα, ένας web εξυπηρετητής μπορεί να έχει ρυθμιστεί έτσι ώστε να έχει πρόσβαση σε αρχεία ενός συγκεκριμένου καταλόγου, αλλά ένας χρήστης να εγκαταστήσει, ηθελημένα ή όχι, ένα CGI script που να επιτρέπει την ανάγνωση κάθε αρχείου στον υπολογιστή.
Η σύνταξη των CGI scripts πρέπει να γίνεται με ιδιαίτερη προσοχή. Οι περισσότεροι χρήστες δεν έχουν εμπειρία στη σύνταξη ασφαλών CGI scripts και συνεπώς υπάρχει υψηλή πιθανότητα να περιέχουν αδυναμίες, επιτρέποντας έτσι σε εισβολείς να εκτελέσουν οποιαδήποτε εντολή στο σύστημα του web εξυπηρετητή.
Τα κενά στην ασφάλεια του web εξυπηρετητή, που δημιουργούνται από τα λάθη ή

την άγνοια των χρηστών, μπορεί να έχουν δυσάρεστες συνέπειες τόσο για τον ίδιο τον εξυπηρετητή όσο και για την ακεραιότητα των αρχείων που φυλάσσονται σε αυτόν. Κάποια ενδεικτικά προβλήματα που είναι πιθανό να παρουσιαστούν είναι τα εξής:

- Ένας εισβολέας μπορεί να εκμεταλλευτεί ατέλειες του web εξυπηρετητή ή των CGI scripts για να αποκτήσει μη εγκεκριμένη πρόσβαση σε αρχεία του εξυπηρετητή, να επέμβει στον εξυπηρετητή τροποποιώντας το σύστημα και να θέσει τον εξυπηρετητή σε προσωρινή αχρηστία.
- Εμπιστευτικές πληροφορίες που βρίσκονται αποθηκευμένες στον web εξυπηρετητή μπορεί να διανεμηθούν σε μη εξουσιοδοτημένα άτομα.
- Εμπιστευτικές πληροφορίες που ανταλλάσσονται μεταξύ του εξυπηρετητή διαδικτύου και του προγράμματος πλοήγησης μπορεί να υποκλαπούν ή να υπάρξει παρεμπόδιση στην αποστολή των δεδομένων, σε οποιοδήποτε σημείο της διαδρομής μεταξύ του εξυπηρετητή και του προγράμματος πλοήγησης.
- Η εμπιστευτικότητα των ηλεκτρονικών συναλλαγών πληρωμής είναι ένα από τα σημαντικότερα ζητήματα ασφάλειας στο ηλεκτρονικό εμπόριο και, σύμφωνα με τα παραπάνω, απαιτείται ένα υψηλό επίπεδο ασφάλειας στον web εξυπηρετητή.

4.2.4 Πολιτική Ασφάλειας.

Για την ασφάλεια του web εξυπηρετητή και κατ'επέκταση για την ασφάλεια όλου του δικτύου, πρέπει να υπάρχει ένα ολοκληρωμένο σύστημα προστασίας. Η υλοποίηση του ανατίθεται στο διαχειριστή του εξυπηρετητή. Για την κατασκευή ενός ασφαλούς web εξυπηρετητή σε οποιαδήποτε πλατφόρμα, πρέπει να ληφθούν υπόψη τα εξής:

- Οι χρήστες του δικτύου δεν πρέπει σε καμιά περίπτωση να μπορούν να εκτελούν προγράμματα ή εντολές κελύφους στον υπολογιστή όπου στεγάζεται ο εξυπηρετητής.
- Τα CGI scripts που τρέχουν στον εξυπηρετητή πρέπει να είναι ελεγμένα διεξοδικά ώστε να επιτελούν τη λειτουργία για την οποία προορίζονται.
- Στην περίπτωση που ο εξυπηρετητής δεχθεί επίθεση, ο επιτιθέμενος δε θα πρέπει να είναι σε θέση να τον χρησιμοποιήσει για να εξαπολύσει επιθέσεις εναντίον των υπόλοιπων υπολογιστών του δικτύου.

Για να ελαχιστοποιηθεί ο κίνδυνος της παρακολούθησης της επικοινωνίας πολλοί οργανισμοί ηλεκτρονικού εμπορίου αγοράζουν ασφαλείς web εξυπηρετητές, που βασίζονται σε κρυπτογραφικά πρωτόκολλα. Αλλά αυτοί οι εξυπηρετητές απαιτούν ψηφιακά υπογεγραμμένα πιστοποιητικά για να λειτουργήσουν και τα πιστοποιητικά αυτά πρέπει να ανανεώνονται τακτικά γεγονός που καθιστά τους εξυπηρετητές ευάλωτους στις επιθέσεις "άρνησης υπηρεσίας".

Ένας οργανισμός ηλεκτρονικού εμπορίου για την υλοποίηση του συστήματος προστασίας θα πρέπει να εφαρμόσει μια πολιτική ασφάλειας σύμφωνα με τους κανονισμούς της ΑΔΑΕ. Η εν λόγω πολιτική ασφάλειας είναι καλό να συμπεριλάβει και παράγοντες όπως:

- Ποιοι επιτρέπεται να χρησιμοποιούν το δίκτυο.
- Πότε επιτρέπεται να το χρησιμοποιούν.

- Τι επιτρέπεται να κάνουν.

Είναι πιθανό διαφορετικές ομάδες χρηστών να έχουν διαφορετικά δικαιώματα εισόδου στα διάφορα μέρη του web εξυπηρετητή. Επίσης οι διαδικασίες παροχής εισόδου στο σύστημα και οι διαδικασίες ανάκλησης της εισόδου, όταν για παράδειγμα ένας χρήστης φεύγει από το σύστημα, αποτελούν ένα σημαντικό κομμάτι του συστήματος προστασίας.
Ένα ακόμη σημείο το οποίο πρέπει να ληφθεί υπόψη είναι το πώς ορίζεται η αποδεκτή χρήση του συστήματος. Ακόμη, στο σύστημα προστασίας, πρέπει να συμπεριληφθούν οι μέθοδοι εισόδου (login) σε αυτό, τόσο για τους εσωτερικούς όσο και για τους εξωτερικούς χρήστες. Τέλος ιδιαίτερο βάρος πρέπει να δοθεί στα πρωτόκολλα που αφορούν τις αντιδράσεις του συστήματος σε τυχόν κενά ασφάλειας.

4.2.5 Ασφάλεια Συστήματος και Λογισμικού των Web Εξυπηρετητών.

Στο εμπόριο και το διαδίκτυο υπάρχουν πολλά λειτουργικά συστήματα. Μερικά από αυτά είναι πιο ασφαλή και μπορούν να χρησιμοποιηθούν ως πλατφόρμες για web εξυπηρετητές. Όσο πιο ευέλικτο και δυναμικό είναι ένα σύστημα τόσο πιο ευάλωτο είναι στις επιθέσεις κατά του εξυπηρετητή. Επίσης, όσα περισσότερα χαρακτηριστικά χρήσης και ευκολίας προσφέρει ο εξυπηρετητής τόσο πιο πιθανό είναι να περιέχει κενά στην ασφάλεια του.
Οι εισβολείς υπολογιστών συνεχώς αναζητούν λάθη σε λογισμικό εξυπηρετητή γιατί κάθε λάθος αναπαριστά μια πιθανή πόρτα εισόδου. Κατασκευάζοντας με προσοχή τα δεδομένα εισόδου που δίνονται στον εξυπηρετητή, ο πονηρός εισβολέας μπορεί να ξεγελάσει το λογισμικό ώστε να πραγματοποιήσει μια μη εγκεκριμένη ενέργεια.
Το πιο ασφαλές σύστημα για web εξυπηρετητή είναι ένας υπολογιστής που τρέχει αποκλειστικά τον εξυπηρετητή και καμιά άλλη εφαρμογή. Παρόλο που ο βασικός εξυπηρετητής του διαδικτύου μπορεί να είναι αρκετά μικρός, αφού χρειάζεται μόνο να ακούει τις εισερχόμενες αιτήσεις για URL, να ανακτά τα αντίστοιχα αρχεία από το δίσκο και να τα στέλνει στο δίκτυο, οι μοντέρνοι web εξυπηρετητές είναι οτιδήποτε παρά απλοί. Οι απλοί εξυπηρετητές που περιέχουν μόνο τα στατικά αρχεία αιτήσεων και καμιά άλλη εφαρμογή θεωρούνται ασφαλέστεροι από τους πολύπλοκους εξυπηρετητές που εκτελούν CGI scripts, αλληλεπιδρούν με μια ποικιλία βάσεων δεδομένων, υποστηρίζουν τις απομακρυσμένες συνδέσεις και προσφέρουν χαρακτηριστικά όπως η λίστα των directories ή τα περιεχόμενα του εξυπηρετητή.

Το λειτουργικό σύστημα UNIX θεωρείται ως μη βέλτιστη επιλογή για web εξυπηρετητή λόγω:

1. Της πληθώρας των γλωσσών προγραμματισμού.
2. Των εσωτερικά σε αυτό εγκαταστημένων εξυπηρετητών.
3. Της πλούσιας ποικιλίας εργαλείων
4. Της ικανότητας σύνδεσης πολλών χρηστών την ίδια στιγμή από οποιοδήποτε απομακρυσμένο σημείο του διαδικτύου.
5. Υπάρχουν πολλοί τρόποι εισόδου στο σύστημα, και είναι εύκολο για τους εισβολείς να εισβάλουν σε αυτό.

Με το σκεπτικό αυτό, λιγότερο ικανά συστήματα, με περιορισμένα εργαλεία και ευκολίες, όπως τα MS-WINDOWS και τα MACINTOSH, είναι δυσκολότερο να δεχθούν επίθεση και επομένως πιο κατάλληλα για web εξυπηρετητές. Ο βασικός λόγος που τα MACINTOSH είναι ασφαλές είναι λόγω του ότι δεν έχουν ερμηνευτή εντολών, στην πλειοψηφία τους δεν εκτελούν οποιαδήποτε υπηρεσία δικτύου και γενικά οι προκαθορισμένες δυνατότητες τους είναι περιορισμένες. Βέβαια το σύστημα UNIX είναι πιο γρήγορο λειτουργικό από το MacOS και είναι διαθέσιμο για πλατφόρμες που είναι πιο γρήγορες από αυτές που χρησιμοποιούν MSWINDOWS. Όσοι επιλέγουν να τρέξουν έναν εξυπηρετητή Window NT ή UNIX έχουν τα πλεονεκτήματα που προσφέρει ένα σύστημα πολυπρογραμματισμού (multitasking). Στο σύνολο τους τα Window NT είναι τρωτά. Αυτό συμβαίνει γιατί το σύστημα αρχείων NT και το σύστημα λογαριασμών των χρηστών είναι αρκετά περίπλοκο και δύσκολο να ρυθμιστεί.
Μερικές από τις προφυλάξεις που πρέπει να λαμβάνονται όταν οι web εξυπηρετητές τρέχουν σε περιβάλλον UNIX ή NT είναι: περιορισμός των λογαριασμών εισόδου (login) που είναι διαθέσιμοι στο σύστημα, διαγραφή των μη ενεργών χρηστών, κλείσιμο των μη απαραίτητων ή μη χρησιμοποιούμενων υπηρεσιών του συστήματος και συχνός έλεγχος των αρχείων πρόσβασης (log files) του εξυπηρετητή και του συστήματος για ύποπτες ενέργειες.
Σε γενικές γραμμές η εμπειρία των ανθρώπων που διαχειρίζονται τον κεντρικό υπολογιστή του εξυπηρετητή και το λογισμικό είναι η πιο σημαντική παράμετρος στην ασφάλεια του συστήματος. Ένα σύστημα UNIX το οποίο διαχειρίζεται ένας έμπειρος χρήστης είναι πιο ασφαλές από ένα MS-WINDOWS σύστημα που διαχειρίζεται κάποιος αρχάριος.

4.2.6 Μέτρα Ασφάλειας.

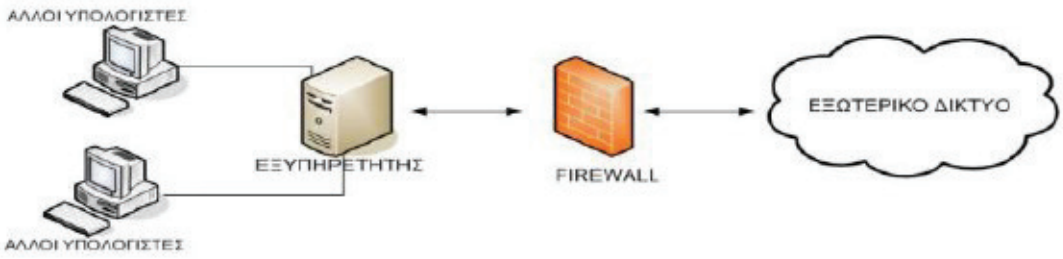
4.2.6.1 Χρήση του Υπολογιστή μόνο από τον Web Εξυπηρετητή.

Όταν ένας υπολογιστής χρησιμοποιείται αποκλειστικά ως web εξυπηρετητής, η ασφάλεια του δικτύου αυξάνεται. Κάτι τέτοιο κάνει πιο δύσκολη την έναρξη επιτυχημένης επίθεσης κατά του μηχανήματος. Αλλά ακόμη και αν ο επιτιθέμενος εισβάλει στο μηχάνημα, δε θα μπορεί να κάνει επιπλέον ζημιά στο δίκτυο. Στην περίπτωση ενός υπολογιστή που λειτουργεί μόνο ως web εξυπηρετητής, συνίσταται η υιοθέτηση των παρακάτω κανόνων:

- Διαγραφή όλων των άχρηστων λογαριασμών.
- Διαγραφή όλων των προγραμμάτων που δε χρησιμοποιούνται από τον web εξυπηρετητή ή από το λογισμικό του μηχανήματος κατά την εκκίνηση του.
- Παροχή των απαιτούμενων υπηρεσιών και μόνο αυτών.
- Μη υποστήριξη υπηρεσιών εξυπηρετητή ηλεκτρονικού ταχυδρομείου (email server).
- Διαγραφή όλων των μεταφραστών γλωσσών (compilers).

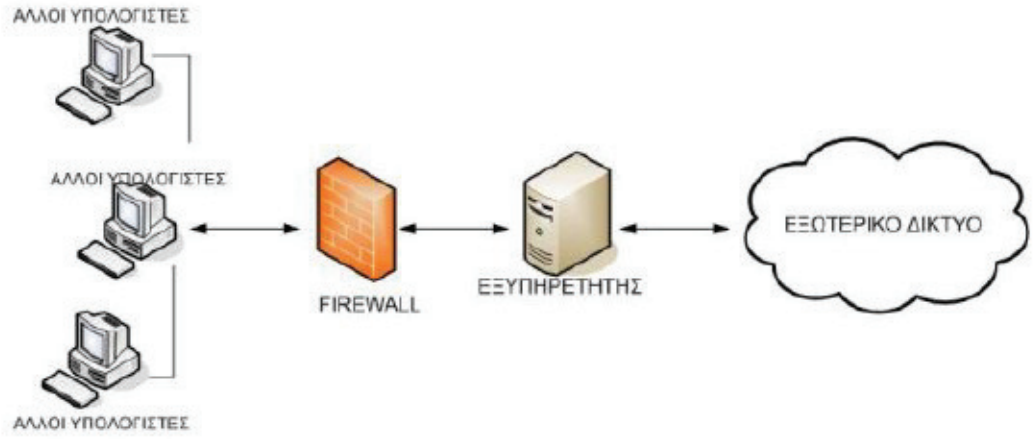
4.2.6.2 Συστήματα Firewalls.

Πολλά δίκτυα για να αυξήσουν την ασφάλεια των ιστοσελίδων τους χρησιμοποιούν firewalls. Τα firewalls είναι ισχυρά εργαλεία τα οποία όμως δεν υποκαθιστούν σε καμιά περίπτωση άλλα μέτρα ασφαλείας και για το λόγο αυτό χρησιμοποιούνται ως συμπληρωματικά αυτών. Συνήθως τοποθετούνται ανάμεσα στο εσωτερικό και στο εξωτερικό δίκτυο ενός οργανισμού και παρέχουν έναν απλό τρόπο για να ελέγχουν την ποσότητα και το είδος των δεδομένων που διακινούνται μεταξύ των δύο δικτύων. Αν το ζητούμενο αποτέλεσμα είναι η δημιουργία ενός εσωτερικού δικτυακού τόπου στο οποίο θα έχουν πρόσβαση μόνο οι χρήστες του τοπικού δικτύου, τότε ο εξυπηρετητής τοποθετείται μέσα στο firewall



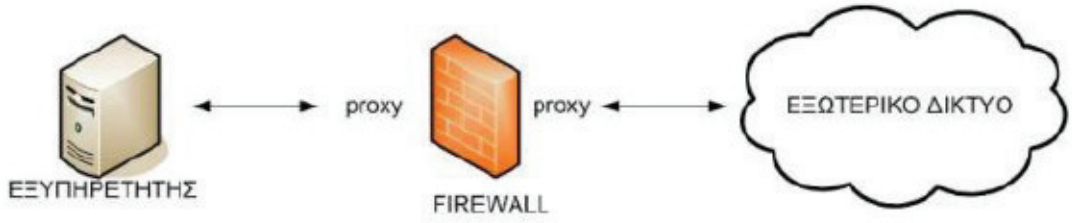
Αν πάλι το ζητούμενο αποτέλεσμα είναι να είναι ο εξυπηρετητής διαθέσιμος στον έξω κόσμο, τότε θα πρέπει να τοποθετηθεί κάπου έξω από το firewall. Για την ασφάλεια και του τοπικού δικτύου θα πρέπει να τοποθετηθεί έξω και από την περιοχή του τοπικού δικτύου.
Η τεχνική αυτή ονομάζεται “διαμόρφωση εξιλαστήριου θύματος” (sacrificial lamb

configuration) διότι ο εξυπηρετητής πάντα κινδυνεύει να καταρρεύσει από επιθέσεις, αλλά με αυτόν τον τρόπο δε θα κινδυνεύει το εσωτερικό δίκτυο ακόμα και αν ο εξυπηρετητής καταρρεύσει. Βέβαια υπάρχουν αρχιτεκτονικές όπου χρησιμοποιούνται ζεύγη εξυπηρετητών (εσωτερικοί και εξωτερικοί) ώστε και στον έξω κόσμο να παρέχουν πληροφορίες και να επιτρέπουν μόνο στους εσωτερικούς χρήστες την πρόσβαση σε ιδιωτικά έγγραφα.
Εάν ο εξυπηρετητής βρίσκεται πίσω από το firewall, υπάρχει τρόπος ώστε να εξασφαλιστεί πρόσβαση στον έξω κόσμο. Με τον τρόπο αυτό, όμως, δημιουργούνται οπές στο φράγμα ασφάλειας. Είναι πολύ καλύτερα να χρησιμοποιηθεί ο εξυπηρετητής ως εξιλαστήριο θύμα. Υπάρχουν βέβαια και αρκετές αρχιτεκτονικές firewalls που δεν επιτρέπουν την τοποθέτηση εξυπηρετητών έξω από αυτούς. Σε αυτή την περίπτωση θα πρέπει αναγκαστικά ο εξυπηρετητής να βρίσκεται πίσω από το φράγμα ασφάλειας με δεδομένο πάντα το μειονέκτημα της πιθανής δημιουργίας οπών ασφάλειας.



Υπάρχουν δύο τρόποι για να επιτευχθεί η πρόσβαση του εξυπηρετητή, που βρίσκεται πίσω από το φράγμα ασφάλειας, με τον έξω κόσμο:

- Στην περίπτωση που χρησιμοποιείται ο τύπος firewall υπολογιστή διαλογής (screened host), μπορεί να επιτραπεί η είσοδος για αιτήσεις (requests) από τη θύρα 80 (http service) η οποία επικοινωνεί με τον web εξυπηρετητή. Έτσι δημιουργείται μια μικρή οπή ασφάλειας απ' όπου ο έξω κόσμος επικοινωνεί με τον εξυπηρετητή.
- Στην περίπτωση που χρησιμοποιείται ο τύπος διπλοσυνδεδεμένο firewall (dual homed gateway), χρειάζεται η εγκατάσταση proxy στο firewall. Ο proxy μπορεί να δει και από τις δύο πλευρές του φράγματος ασφάλειας, όπως φαίνεται στο Σχήμα .Έτσι, οι αιτήσεις για πληροφορίες σταματούν πάνω στον proxy ο οποίος τις προωθεί στον εξυπηρετητή και οι απαντήσεις από τον εξυπηρετητή σταματούν στον proxy ο οποίος τις προωθεί στον αιτούντα.



4.2.6.3 Προστασία Εμπιστευτικών Αρχείων.
Πολλοί οργανισμοί ηλεκτρονικού εμπορίου επιθυμούν να περιορίσουν τις πληροφορίες που θα διανείμουν οι εξυπηρετητές τους, αφού κάποιοι web εξυπηρετητές χρησιμοποιούνται για τη διανομή δεδομένων εμπιστευτικής φύσεως. Τέτοια δεδομένα είναι πληροφορίες για τις ηλεκτρονικές συναλλαγές, όπως τα προσωπικά στοιχεία του πελάτη, τα στοιχεία της συναλλαγής ή πληροφορίες για τους εργαζόμενους του οργανισμού. Για την ικανοποίηση αυτής της απαίτησης, πολλοί web εξυπηρετητές παρέχουν τρόπους προστασίας των εμπιστευτικών εγγράφων. Υπάρχουν τρεις τρόποι περιορισμού της πρόσβασης:

- Περιορισμός πρόσβασης σύμφωνα με τις IP διευθύνσεις, υποδίκτυα (subnets), ή τα ονόματα πεδίων (domain names): Έγγραφα και κατάλογοι προστατεύονται με τέτοιο τρόπο ώστε μόνο τα προγράμματα πλοήγησης που συνδέονται από συγκεκριμένες IP διευθύνσεις, IP υποδίκτυα, ή πεδία (domains) να έχουν πρόσβαση σε αυτά.
- Περιορισμός πρόσβασης σύμφωνα με ονόματα χρηστών και κωδικών: Έγγραφα και κατάλογοι προστατεύονται με τέτοιο τρόπο ώστε ο απομακρυσμένος χρήστης για να αποκτήσει πρόσβαση σε αυτά να πρέπει να χρησιμοποιήσει κατάλληλο όνομα και κωδικό
- Κρυπτογράφηση με χρήση ασύμμετρης κρυπτογραφίας: Η αίτηση για το έγγραφο και το ίδιο το έγγραφο μεταδίδονται κρυπτογραφημένα, ώστε μόνο ο πραγματικός παραλήπτης να μπορεί να τα διαβάσει. Χρησιμοποιούνται δημόσια κλειδιά και πιστοποιητικά. Αυτό το είδος περιορισμού παρέχεται μόνο από τους εξυπηρετητές που είναι εξοπλισμένοι με το απαραίτητο λογισμικό.

Κάθε μια από τις παραπάνω τεχνικές έχει πλεονεκτήματα και μειονεκτήματα. Ο περιορισμός μέσω των IP διευθύνσεων έχει αποτέλεσμα σε περιπτώσεις απλών χρηστών, αλλά όχι απέναντι σε αποφασισμένους εισβολείς. Με κατάλληλο εξοπλισμό και λογισμικό, ένας εισβολέας μπορεί να αλλάξει την IP διεύθυνση του (IP spoofing) και να εμφανίζεται ως συνδεδεμένος από κάπου αλλού. Επίσης, ο απομακρυσμένος υπολογιστής μπορεί να έχει καταληφθεί και να χρησιμοποιείται ως βιτρίνα. Ο περιορισμός μέσω των IP διευθύνσεων μπορεί να γίνει ασφαλέστερος αν ο εξυπηρετητής προστατεύεται από ένα firewall που είναι ικανό να εντοπίζει και να απορρίπτει τις προσπάθειες για αλλαγή των IP διευθύνσεων. Οι περιορισμοί μέσω υπολογιστή φιλοξενίας (host) ή ονόματος πεδίου (domain) εμφανίζουν τα ίδια προβλήματα με τους περιορισμούς μέσω IP διευθύνσεων. Για μέγιστη ασφάλεια, η

τεχνική αυτή πρέπει να συνδυάζεται με τον έλεγχο της ταυτότητας του χρήστη.
Ο περιορισμός μέσω μυστικών κωδικών έχει και αυτός κάποια προβλήματα. Οι κωδικοί που επιλέγουν οι χρήστες δεν είναι πάντοτε ασφαλείς. Πολύ συχνά χρησιμοποιούν φανερούς κωδικούς όπως ονόματα, ημερομηνίες γέννησης, τηλέφωνα. Τέτοιοι κωδικοί είναι προβλέψιμοι και οι web εξυπηρετητές δεν απαγορεύουν τις επανειλημμένες αποτυχημένες προσπάθειες εισαγωγής του σωστού κωδικού. Ένας εισβολέας μπορεί να εφαρμόσει ένα πρόγραμμα υπόθεσης κωδικών (password guessing program) και να υποθέσει το σωστό κωδικό. Ένα άλλο πρόβλημα με τους κωδικούς είναι ότι είναι ευάλωτοι σε υποκλοπή καθώς μεταδίδονται στο δίκτυο. Επειδή δεν είναι ισχυρά κρυπτογραφημένοι, ένας εισβολέας μπορεί με κατάλληλο υλικό και λογισμικό να τους καταγράψει και να τους χρησιμοποιήσει μελλοντικά .Επιπλέον το πρόγραμμα πλοήγησης στέλνει τον κωδικό στον εξυπηρετητή κάθε φορά που ζητά κάποιο εμπιστευτικό έγγραφο, διευκολύνοντας έτσι τον εισβολέα να υποκλέψει τον κωδικό αυτό.
Ο συνδυασμός όλων των παραπάνω τεχνικών αποτελεί την καλύτερη δυνατή λύση. Με τον περιορισμό των IP διευθύνσεων και των ονομάτων πεδίων περιορίζεται ο αριθμός των υπολογιστών που μπορεί να έχουν πρόσβαση στον εξυπηρετητή, ενώ με τον περιορισμό μέσω κωδικών πρόσβασης περιορίζονται οι χρήστες που έχουν το δικαίωμα να αποκτήσουν πρόσβαση στα εμπιστευτικά αρχεία. Τέλος, με την κρυπτογράφηση, διασφαλίζεται η εμπιστευτικότητα των πληροφοριών που ανταλλάσσονται.

4.2.7 Web Εξυπηρετητές και Εμπόριο.

Στο ηλεκτρονικό εμπόριο κυριαρχούν τρεις web εξυπηρετητές, των οποίων τα κύρια χαρακτηριστικά παρουσιάζονται παρακάτω:

Apache server.
- Η απλή του έκδοση είναι δωρεάν, αλλά όχι αυτή με ασφάλεια SSL.
- Εκτελείται καλύτερα σε περιβάλλον UNIX.
- Απαιτείται εμπειρία στοUNIX για να εγκατασταθεί-διαχειριστεί.
- Υποστηρίζεται από εργαλεία τρίτων κατασκευαστών.

Microsoft Internet Information Server (IIS).
- Περιλαμβάνεται στα Windows NT/2000.
- Εύκολη διαχείριση.
- Προσφέρει περιβάλλον ανάπτυξης εφαρμογών.
- Πολύ καλές επιδόσεις.

Netscape Enterprise Server.
- Ευκολία εγκατάστασης και διαχείρισης.
- Δυνατότητες εξυπηρέτησης μέχρι 100 εκατομμύρια αιτήσεων την ημέρα.
- Υποστηρίζεται από UNIX και Windows.

4.2.8 Ασφάλεια Web Εφαρμογών.

Ο όρος ασφάλεια περιλαμβάνει την προστασία των αγαθών (assets) των επιχειρήσεων. Τα αγαθά μπορεί να είναι απτά στοιχεία, όπως μια ιστοσελίδα ή η βάση δεδομένων των πελατών της επιχείρησης, ή μπορεί να είναι λιγότερο απτά, όπως η φήμη της εταιρείας.

4.2.8.1 Απαιτήσεις Ασφάλειας.

Οι βασικές απαιτήσεις για την ασφάλεια των web εφαρμογών είναι οι εξής:

Αυθεντικοποίηση (Authentication): Η διαδικασία της αυθεντικοποίησης αποσκοπεί στην εξακρίβωση της ταυτότητας, την οποία ισχυρίζεται ότι έχει ένας πελάτης της εφαρμογής. Ο πελάτης μπορεί να είναι κάποιος τελικός χρήστης, κάποια υπηρεσία, διαδικασία ή υπολογιστής. Στο ηλεκτρονικό εμπόριο η πιστοποίηση της ταυτότητας των μερών που συμμετέχουν σε μια συναλλαγή είναι απαραίτητη ώστε, κάθε συναλλασσόμενο μέρος να είναι σίγουρο για την ταυτότητα του άλλου.Ο έλεγχος αυθεντικότητας παρέχεται συνήθως μέσω ψηφιακών υπογραφών.

Εμπιστευτικότητα (Confidentiality): Είναι έννοια στενά συνδεδεμένη με την ιδιωτικότητα (privacy) και τη μυστικότητα (secrecy). Αφορά τη μη αποκάλυψη των ευαίσθητων πληροφοριών σε άτομα που δεν έχουν την κατάλληλη εξουσιοδότηση.Για το ηλεκτρονικό εμπόριο η εμπιστευτικότητα αποτελεί υψίστης σημασίας συστατικό στην προστασία των οικονομικών δεδομένων του οργανισμού, καθώς και στην προστασία των προσωπικών δεδομένων των πελατών. Τεχνικές κρυπτογράφησης χρησιμοποιούνται για να εξασφαλίσουν την εμπιστευτικότητα.

Εξουσιοδότηση (Authorization): Η εξουσιοδότηση περιλαμβάνει τον έλεγχο πρόσβασης σε συγκεκριμένες πληροφορίες και υπηρεσίες όταν η ταυτότητα του χρήστη εξακριβωθεί. Η εξουσιοδότηση στην ουσία περιορίζει τις ενέργειες ή τις λειτουργίες που τα εξουσιοδοτούμενα μέλη μπορούν να πραγματοποιήσουν, όπως για παράδειγμα εκτέλεση συναλλαγών, μεταφορά χρημάτων από ένα λογαριασμό σε άλλο ή αύξηση του πιστωτικού ορίου κάποιου πελάτη.

Ακεραιότητα (Integrity): Η ακεραιότητα είναι η εγγύηση ότι τα δεδομένα προστατεύονται από τυχαία ή σκόπιμη (κακόβουλη) τροποποίηση. Διασφαλίζει την εγκυρότητα, την ορθότητα και την πληρότητα των δεδομένων κατά τη φάση της εισαγωγής τους, της αποθήκευσης και της μεταφοράς τους. Τα συστήματα ηλεκτρονικού εμπορίου πρέπει να χρησιμοποιούν τέτοιες μεθόδους ώστε να μπορούν να διασφαλίσουν ότι τα δεδομένα φτάνουν στον προορισμό τους όπως ακριβώς στάλθηκαν.

Μη αποποίηση ευθύνης (Non- repudiation): Μη αποποίηση ευθύνης σημαίνει ότι

ένας χρήστης δεν μπορεί να αρνηθεί την εκτέλεση μιας λειτουργίας, και κανένα από τα συναλλασσόμενα μέρη δεν έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή. Οι υπηρεσίες μη αποποίησης ευθύνης πρέπει, σε περίπτωση που χρειαστεί, να μπορούν να αποδείξουν την προέλευση, μεταφορά και παραλαβή των δεδομένων.

Διαθεσιμότητα (Availability): Αφορά την άμεση πρόσβαση στις υπηρεσίες του συστήματος για τους νόμιμους χρήστες του. Πολλοί επιτιθέμενοι, χρησιμοποιώντας επιθέσεις τύπου άρνησης υπηρεσίας (denial of service), έχουν σαν στόχο να συντρίψουν την εφαρμογή, ώστε οι υπόλοιποι χρήστες να μην μπορούν να έχουν πρόσβαση στην συγκεκριμένη εφαρμογή.

4.2.8.2 Επίδραση στο Επιχειρησιακό Περιβάλλον.

Οι κίνδυνοι ασφάλειας εφαρμογών που προκύπτουν από την αποθήκευση και την επεξεργασία των επιχειρηματικών πληροφοριών από τις εκάστοτε εφαρμογές, αφορούν στην απώλεια της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών. Η σημαντικότητα των κινδύνων αυτών προσδιορίζεται από την επίδραση τους στο επιχειρησιακό περιβάλλον και από την πιθανότητα εκδήλωσης τους.
Η επίδραση από την απώλεια της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών είναι:
- Απώλεια ανταγωνιστικού πλεονεκτήματος.
- Αδυναμία διεκπεραίωσης βασικών επιχειρηματικών δραστηριοτήτων.
- Προσβολή της εμπιστοσύνης των πελατών προς την εταιρεία.
- Προσβολή της εικόνας και της φήμης της εταιρείας.
- Αδυναμία επαναλειτουργίας λόγω πολλών ανεκτέλεστων διαδικασιών οι οποίες δεν μπορούν να εκτελεστούν είτε λόγω χρονικού περιορισμού, είτε επειδή έχουν χαθεί.
- Πιθανότητα απάτης.
- Αδυναμία λειτουργίας λόγω απώλειας διαθεσιμότητας των πληροφοριακών πόρων.

4.2.8.3 Εχθροί, Απειλές και Επιθέσεις

Απειλή είναι οποιοδήποτε πιθανό περιστατικό, κακόβουλο ή όχι, που μπορεί να βλάψει κάποιο αγαθό. Με άλλα λόγια, απειλή είναι οτιδήποτε κακό μπορεί να συμβεί στα αγαθά. Ευπάθεια είναι μια αδυναμία που κάνει δυνατή την απειλή. Αυτό μπορεί να γίνει λόγω αδυναμιών στη σχεδίαση, λάθη στη διαμόρφωση ή λόγω ακατάλληλων και επισφαλών τεχνικών κωδικοποίησης.
Επίθεση είναι μια ενέργεια που εκμεταλλεύεται τις ευπάθειες και υλοποιεί μια απειλή. Προκειμένου να σχεδιαστεί και να αναπτυχθεί μια ασφαλής web εφαρμογή, απαιτείται η γνώση τόσο των απειλών όσο και των εχθρών του συστήματος. Είναι σημαντικό να αναλυθεί η αρχιτεκτονική της εφαρμογής και να καθοριστούν οι

πιθανές ευπαθείς περιοχές που μπορούν να επιτρέψουν σε ένα χρήστη ή σε έναν επιτιθέμενο με κακόβουλες προθέσεις, να παραβιάσει την ασφάλεια του συστήματος. Παρακάτω ακολουθούν αναλυτικά οι κατηγορίες των εχθρών, παρουσιάζονται οι πιο συνήθεις απειλές καθώς και οι τεχνικές επιθέσεων που κάνουν πραγματικότητα αυτές τις απειλές.

Εχθροί.

Είναι σημαντικό στην προσπάθεια παροχής ασφάλειας στις εφαρμογές ηλεκτρονικού εμπορίου, να αναγνωρίζονται αρχικά «εχθροί». Οποιοσδήποτε εμπλέκεται με ζητήματα ασφάλειας ηλεκτρονικού εμπορίου θα πρέπει να τον απασχολούν οι εχθροί του συστήματος, οι προθέσεις τους καθώς και τα μέσα που διαθέτουν. Οι «εχθροί» κατηγοριοποιούνται ως εξής:

Crackers: Οι crackers αρέσκονται στο δημιουργούν προβλήματα για πλάκα, για βανδαλισμούς ή για επίδειξη. Χρησιμοποιούν συνήθως υπάρχοντα προϊόντα επίθεσης από το διαδίκτυο. Οι προθέσεις τους συχνά δεν είναι εχθρικές, αλλά ωστόσο προκαλούν ουσιαστικές ζημιές, είτε προκαλώντας βανδαλισμούς, είτε διακόπτοντας λειτουργίες.

Ερευνητές (Researchers): Ένας ερευνητής μπορεί να εργαστεί πολύ σκληρά στην προσπάθεια του να ανακαλύψει αδυναμίες σε πρωτόκολλα ασφάλειας και στη συνέχεια εκδίδει τα αποτελέσματα του στο διαδίκτυο.

Εγκληματίες (Criminals): Το διαδίκτυο έχει γίνει πολύ ελκυστικό μέρος για εγκλήματα, λόγω της μεγάλης διάδοσης και ανωνυμίας που παρέχει. Το δικτυακά εγκλήματα εκτείνονται από απλές απάτες με κλοπή αριθμών πιστωτικών καρτών έως προσεκτικές επιθέσεις για πρόσβαση σε χρήμα ή πληροφορίες. Πρόθεση τους είναι το οικονομικό όφελος.

Ανταγωνιστές (Competitors): Ένας ανταγωνιστής δεν κλέβει χρήματα, ούτε καταστρέφει αρχεία, αλλά έχει ως στόχο την πρόσβαση στα διάφορα επιχειρηματικά σχέδια, που είναι πολύτιμα για αυτόν.

Εσωτερικοί εχθροί: Δυσαρεστημένοι ή άπληστοι υπάλληλοι μπορούν να αποτελέσουν την πιο σοβαρή απειλή για την ασφάλεια των συστημάτων του οργανισμού. Οι «εσωτερικοί εχθροί» εξ ορισμού έχουν πρόσβαση σε ευαίσθητα συστήματα και πληροφορίες.

Απειλές.

Οι θεμελιώδεις απειλές που αντιμετωπίζουν οι web εφαρμογές είναι:

- Διαρροή πληροφοριών (information leakage).
- Παραβίαση της ακεραιότητας των πληροφοριών (integrity violation).
- Διακοπή υπηρεσιών.
- Άρνηση εξυπηρέτησης (denial of services).

- Πρόσβαση χωρίς εξουσιοδότηση σε δικτυακούς πόρους.
- Κλοπή δεδομένων.
- Παράνομη χρήση διάφορων υπολογιστικών πόρων.
- Καταστροφή πληροφοριών και δικτυακών πόρων.

Επιθέσεις.

Η πραγματοποίηση οποιασδήποτε από τις παραπάνω θεμελιώδεις απειλές, μπορεί να γίνει με μια από τις παρακάτω τεχνικές επίθεσης:

Denial of service attacks: Μια από τις πλέον διάσημες και αποτελεσματικές μεθόδους που χρησιμοποιούν οι επιτιθέμενοι με στόχο τη διακοπή παροχής υπηρεσιών από ένα δικτυακό κόμβο ή πληροφοριακό σύστημα είναι οι επιθέσεις τύπου Denial of service. Τα προγράμματα που συνήθως χρησιμοποιούν οι επιτιθέμενοι ακολουθούν την τακτική μαζικής αποστολής μηνυμάτων- αιτημάτων στο στόχο ώστε να προκαλέσουν την αποτυχία ανταπόκρισης του και την κατάρρευση του συστήματος.

Επιθέσεις μεταμφίεσης (Spoofing): Κατά τις επιθέσεις αυτές, ο επιτιθέμενος προσποιείται κάποιον άλλον, «μεταμφιέζεται» σε κάποιο νόμιμο χρήστη, ώστε να αποκτήσει πρόσβαση σε μια εφαρμογή. Δηλαδή ο επιτιθέμενος κάνει χρήση των στοιχείων πρόσβασης ενός εξουσιοδοτημένου χρήστη. Αυτό μπορεί να είναι αποτέλεσμα των εξής: α) οι εξουσιοδοτημένοι χρήστες δεν ακολουθούν τους κανόνες προστασίας των κωδικών πρόσβασης, β) οι κωδικοί πρόσβασης είτε διακινούνται μέσω του δικτύου, είτε αποθηκεύονται χωρίς κρυπτογράφηση, και γ) οι χρήστες χρησιμοποιούν εύκολους κωδικούς.

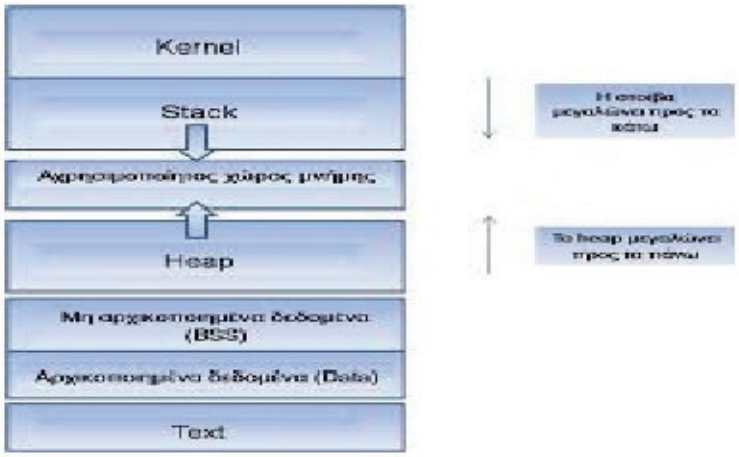
E-mail Spoofing: Το e-mail spoofing αποτελεί πρακτική παραποίησης ή απόκρυψης της πραγματικής πηγής από την οποία προήρθε το μήνυμα ηλεκτρονικού ταχυδρομείου. Χρησιμοποιείται συνήθως για να παραπλανήσει το χρήστη ώστε να συλλεχθούν από αυτόν χρήσιμα δεδομένα. Ενδεικτικά αποστέλλονται μηνύματα με υποτιθέμενο αποστολέα τον διαχειριστή του συστήματος, ζητώντας από το χρήστη να επιβεβαιώσει το password που χρησιμοποιεί.

Επιθέσεις παρακολούθησης (Sniffing): Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων για να αναλύουν τη συμπεριφορά συστημάτων και να εντοπίζουν πιθανά προβλήματα είναι τα λεγόμενα «προγράμματα sniffing». Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο. Οι συσκευές με δυνατότητες sniffing μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης εισβολών IDS (Intrusion Detection System). Συνεπώς τέτοιου είδους συσκευές είναι χρήσιμες και απαραίτητες. Ωστόσο, είναι προφανές ότι οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις υπηρεσίες που προσφέρουν τα προγράμματα sniffing για την υλοποίηση των παράνομων δραστηριοτήτων τους.Υπάρχουν ειδικά προγράμματα

sniffing, ορισμένα από τα οποία είναι δωρεάν, τα οποία μπορούν να χρησιμοποιηθούν για την παρακολούθηση: α) password, β) στοιχείων οικονομικών συναλλαγών (π.χ. κωδικοί πιστωτικών καρτών), γ) εμπιστευτικών δεδομένων (π.χ. προσωπικά στοιχεία χρηστών, e-mail).

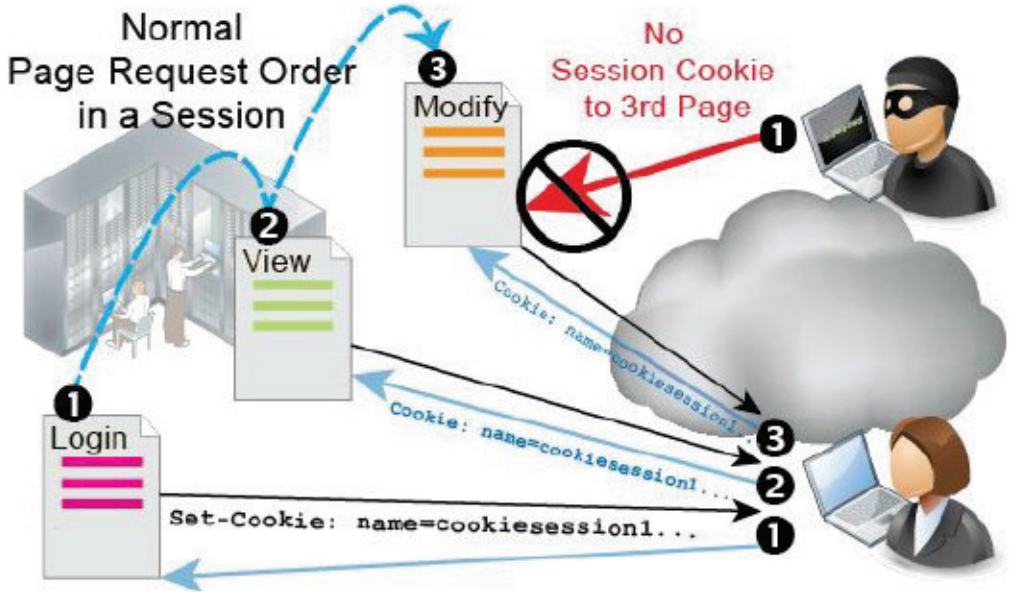
Ιοί (viruses) - σκουλήκια (worms): Οι ιοί είναι προγράμματα ή εντολές που προσαρτώνται σε προγράμματα ή δεδομένα και εκτελούνται παράλληλα με αυτά. Μπορούν να προκαλέσουν την αλλοίωση ή καταστροφή δεδομένων. Τα σκουλήκια αντίστοιχα, είναι προγράμματα που κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Και οι δύο κατηγορίες προγραμμάτων έχουν ως στόχο να πλήξουν το σύστημα στο οποίο εκτελούνται, προκαλώντας ζημιές όπως διαγραφή δεδομένων.

Buffer overflow attacks (υπερχείλιση καταχωρητή): Οι επιθέσεις αυτού του τύπου έχουν σαν στόχο να πλήξουν τις εφαρμογές που αποθηκεύουν δεδομένα σε προσωρινό χώρο μνήμης (buffer) μέχρι να έρθει η ώρα τους για επεξεργασία. Οι επιτιθέμενοι βάζουν κώδικα δικής τους κατασκευής στο πακέτο που στέλνεται για αποθήκευση στον καταχωρητή με σκοπό την αντικατάσταση μέρους του κώδικα της εφαρμογής με τις δικές τους εντολές. Σε περίπτωση επιτυχημένης εκτέλεσης των εντολών, οι επιτιθέμενοι αποκτούν προνόμια πρόσβασης μεγαλύτερα ενός απλού χρήστη της εφαρμογής και καταφέρνουν να αποκτήσουν τον έλεγχο του συστήματος.



Cookie Poisoning: Τα Cookies είναι αρχεία υπολογιστών που αποθηκεύονται στον σκληρό δίσκο του υπολογιστή του πελάτη ή στην μνήμη cache, κατά την πρόσβαση του σε μια εφαρμογή διαδικτύου μέσω ενός browser. Αυτά τα αρχεία περιέχουν πληροφορίες όπως όνομα χρήστη,κωδικός πρόσβασης και στοιχεία συνόδου. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτές τις πληροφορίες με σκοπό τη χρήση του υπολογιστή του πελάτη για κακόβουλες πράξεις. Τα Cookies χωρίζονται σε δύο κατηγορίες: αυτά που μένουν στον υπολογιστή του χρήστη μόνο κατά τη διάρκεια της επίσκεψης του χρήστη στην εφαρμογή διαδικτύου, και αυτά που έχουν ημερομηνία

λήξης και παραμένουν στον σκληρό δίσκο του πελάτη μέχρι την ημερομηνία λήξης τους οπότε και διαγράφονται.



4.2.8.4 Μέσα Προστασίας

Ασφάλεια Δικτύου, Host και Εφαρμογής.

Ο σχεδιασμός και η ανάπτυξη ασφαλών web εφαρμογών προϋποθέτει ότι πρέπει να εφαρμοστεί ασφάλεια και στα τρία στρώματα: Δικτύου (Network), Host και Εφαρμογής (Application).

Ασφάλεια Δικτύου (Network).

Η ασφάλεια μιας web εφαρμογής στηρίζεται πάνω στην ασφαλή υποδομή του δικτύου. Η υποδομή του δικτύου αποτελείται από δρομολογητές (rooters), firewalls και διακόπτες (switches). Ο ρόλος της ασφάλειας δικτύου δεν είναι μόνο για την προστασία του από επιθέσεις βασισμένες στο πρωτόκολλο TCP/IP, αλλά και για την εφαρμογή αντίμετρων όπως ασφαλείς διεπαφές και ισχυροί κωδικοί πρόσβασης. Το ασφαλές δίκτυο είναι επίσης υπεύθυνο για τη διασφάλιση της ακεραιότητας των δεδομένων που διακινούνται μέσα από αυτό.
Τα firewalls μπλοκάρουν τα πρωτόκολλα και τις θύρες που δεν χρησιμοποιεί η εφαρμογή. Επιπλέον εξετάζουν τις επικοινωνίες και παρέχουν υψηλή ασφάλεια στο δίκτυο. Συγκεκριμένα με την εφαρμογή φιλτραρίσματος εμποδίζουν τις κακόβουλες επικοινωνίες. Τα firewalls αποτελούν αναπόσπαστο τμήμα της ασφάλειας, αλλά δεν αποτελούν πλήρη λύση από μόνα τους.

Ασφάλεια Host.

Η ασφάλεια web εφαρμογών προϋποθέτει πρώτα από όλα την ασφάλεια του εξυπηρετητή (server), είτε αυτός είναι εξυπηρετητής διαδικτύου (web server), εξυπηρετητής εφαρμογής (application server) ή εξυπηρετητής βάσεων δεδομένων (database server). Ακολούθως παρατίθενται τα μέτρα προστασίας που πρέπει να λαμβάνονται για την προστασία του εξυπηρετητή, και κατ'επέκταση των web εφαρμογών:

Patches and Updates:

Πολλοί κίνδυνοι ασφάλειας υπάρχουν λόγω του ότι οι ευπάθειες είναι ευρέως

γνωστές και διαδεδομένες. Όταν ανακαλύπτονται νέες ευπάθειες, συχνά ο εκμεταλλευόμενος κώδικας δημοσιεύεται στους πίνακες δελτίων του διαδικτύου μέσα σε λίγες ώρες από την πρώτη επιτυχημένη επίθεση. Η συχνή επιδιόρθωση (patching) και ενημέρωση (updating) του λογισμικού του εξυπηρετητή είναι το πρώτο βήμα για την εξασφάλιση της ασφάλειας στον εξυπηρετητή. Η χρήση των patches και updates στον εξυπηρετητή μειώνει τις ευκαιρίες για επίθεση τόσο των επιτιθέμενων όσο και του κακόβουλου κώδικα (malicious code).

Υπηρεσίες: Η απενεργοποίηση των περιττών και αχρησιμοποίητων υπηρεσιών μειώνει εύκολα και γρήγορα τη διαθέσιμη περιοχή για επιθέσεις (attach surface area).

Πρωτόκολλα: Η απενεργοποίηση των περιττών και αχρησιμοποίητων πρωτοκόλλων μειώνει επίσης τη διαθέσιμη περιοχή για επιθέσεις και τους ανοικτούς «δρόμους» που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι για να εισβάλουν στο σύστημα.

Accounts (Λογαριασμοί): Ο αριθμός των λογαριασμών που έχουν πρόσβαση στον εξυπηρετητή πρέπει να περιοριστεί στον ελάχιστο δυνατό. Επιπλέον θα πρέπει να επιβάλλονται κατάλληλες πολιτικές ασφάλειας των λογαριασμών όπως είναι η εξουσιοδότηση με ισχυρούς κωδικούς πρόσβασης.

Ports (Θύρες): Οι υπηρεσίες που τρέχουν σε έναν εξυπηρετητή ακούνε συγκεκριμένες θύρες προκειμένου να εξυπηρετήσουν τις εισερχόμενες αιτήσεις. Οι ανοικτές θύρες σε έναν εξυπηρετητή πρέπει να είναι γνωστές και να ελέγχονται συχνά ώστε καμιά επισφαλής υπηρεσία να μην ακούει.

Auditing and Logging (Έλεγχος και Καταγραφή): Ο έλεγχος είναι ζωτικής σημασίας στον προσδιορισμό εισβολέων ή επιθέσεων που βρίσκονται σε εξέλιξη. Η καταγραφή αποδεικνύεται ιδιαίτερα χρήσιμη, καθώς αποθηκεύονται πληροφορίες για τον τρόπο που εκτελέστηκε μια επίθεση οι οποίες μπορούν να χρησιμοποιηθούν για ενίσχυση των μέτρων προστασίας ενάντια σε παρόμοιου είδους επιθέσεις.

Ασφάλεια Εφαρμογής. Προκειμένου να εξασφαλιστεί η ασφάλεια των web εφαρμογών ακολουθούνται κάποιες βασικές διαδικασίες οι οποίες είναι οι εξής:

- Επικύρωση δεδομένων εισόδου (Input Validation): Η επικύρωση δεδομένων εισόδου ασχολείται με το πως τα φίλτρα της εφαρμογής δέχονται κάποια δεδομένα εισόδου ως έγκυρα και ασφαλή και κάποια άλλα τα απορρίπτουν ως μη ασφαλή. Αυθεντικοποίηση: Αυθεντικοποίηση είναι η διαδικασία κατά την οποία κάποια οντότητα αποδεικνύει την ταυτότητα κάποιας άλλης οντότητας, συνήθως με τη χρήση πιστοποιητικών.
- Εξουσιοδότηση: Η εξουσιοδότηση αναφέρεται στον τρόπο με τον οποίο η εφαρμογή παρέχει έλεγχο πρόσβασης στις διαδικασίες.
- Διαχείριση Διαμόρφωσης: Η διαχείριση διαμόρφωσης ασχολείται με το πως η εφαρμογή χειρίζεται κάποια λειτουργικά ζητήματα όπως είναι ποιες βάσεις δεδομένων ενώνονται με την εφαρμογή, ή με ποιο τρόπο η εφαρμογή διοικείται.

- Ευαίσθητα Δεδομένα: Τα ευαίσθητα δεδομένα αναφέρονται στο πως η εφαρμογή χειρίζεται τα δεδομένα που πρέπει να προστατευτούν.
- Διαχείριση Συνόδου: Μια σύνοδος αναφέρεται σε μια σειρά σχετικών αλληλεπιδράσεων μεταξύ του χρήστη και της web εφαρμογής. Η διαχείριση συνόδου ασχολείται με το πως η εφαρμογή χειρίζεται και προστατεύει αυτές τις αλληλεπιδράσεις.
- Κρυπτογράφηση: Η κρυπτογράφηση αναφέρεται στο πως η εφαρμογή παρέχει εμπιστευτικότητα και ακεραιότητα.
- Διαχείριση εξαιρέσεων: Η διαχείριση εξαιρέσεων ασχολείται με το τι κάνει η εφαρμογή σε περίπτωση που αποτύχει μια κλήση, δηλαδή αν επιστρέφει φιλικά μηνύματα προς τον χρήστη κλπ.
- Έλεγχος και Καταγραφή: Ο έλεγχος και η καταγραφή αναφέρονται στο πως η εφαρμογή καταγράφει τα σχετικά με την ασφάλεια γεγονότα.

4.2.8.5.Αρχές Ασφάλειας.

Οι βασικές αρχές ασφάλειας πρέπει να εφαρμόζονται σε κάθε είδους εφαρμογές, ανεξάρτητα από την τεχνολογία της κάθε εφαρμογής. Οποιοσδήποτε ασχολείται με την ασφάλεια των web εφαρμογών πρέπει να τηρεί τις παρακάτω βασικές αρχές ασφάλειας:

- Ελάχιστα δυνατά προνόμια: Θα πρέπει να παραχωρούνται στους χρήστες ελάχιστα προνόμια και δικαιώματα πρόσβασης, ούτως ώστε οι επιτιθέμενοι να έχουν περιορισμένες ικανότητες σε περίπτωση που καταφέρουν να παραβιάσουν την ασφάλεια της εφαρμογής.
- Έλεγχος εγκυρότητας εισαγόμενων δεδομένων: Τα δεδομένα τα οποία εισάγονται στην εφαρμογή από τους χρήστες αποτελούν δίοδο εχθρικού λογισμικού προς την εφαρμογή. Τα δεδομένα αυτά αποτελούν το αρχικό όπλο του επιτιθέμενου στην προσπάθεια του να εισβάλει στην εφαρμογή. Τα εισερχόμενα προς την εφαρμογή δεδομένα θα πρέπει να ελέγχονται.Η πιο ασφαλής τακτική ελέγχου είναι να θεωρούνται όλα τα δεδομένα εισαγωγής κακόβουλα μέχρι να αποδειχθεί το αντίθετο και να γίνεται έλεγχος επικύρωσης όλων των δεδομένων, ώστε η εφαρμογή να αποδέχεται μόνο ασφαλή δεδομένα και να απορρίπτει τα υπόλοιπα.
- Έλεγχος στην πύλη: Όλοι οι επισκέπτες θα πρέπει να αυθεντικοποιούνται κατά την είσοδο τους στο σύστημα.
- Αποτυχία με ασφάλεια: Σε περίπτωση που αποτύχει η εφαρμογή τα ευαίσθητα δεδομένα δεν θα πρέπει να παραμένουν προσιτά σε τρίτους. Θα πρέπει να επιστρέφονται φιλικά μηνύματα σφάλματος στους χρήστες τα οποία να μην εκθέτουν τις εσωτερικές λεπτομέρειες του συστήματος και γενικά να μην περιλαμβάνουν λεπτομέρειες που θα μπορούσαν να βοηθήσουν τους επιτιθέμενους να εκμεταλλευτούν τις ευπάθειες τις εφαρμογής.
- Δημιουργία ασφαλών προεπιλογών: Οι λογαριασμοί προεπιλογής (default

account) θα πρέπει εξ ορισμού να είναι εκτός λειτουργίας και σε περίπτωση ανάγκης να επιτρέπεται ρητά η χρήση τους. Όταν εμφανίζεται ένα λάθος θα πρέπει τα ευαίσθητα δεδομένα να μην διαρρέουν πίσω στον χρήστη ο οποίος ενδεχομένως θα μπορεί να τα χρησιμοποιήσει ενάντια στο σύστημα.

- Μείωση περιοχής επιθέσεων: Θα πρέπει να μειώνεται η διαθέσιμη περιοχή για επιθέσεις. Αυτό μπορεί να γίνει θέτοντας εκτός λειτουργίας ή αφαιρώντας αχρησιμοποίητες συσκευές και πρωτόκολλα.

4.2.8.6 Πλάνο Ασφάλειας.

Οι υπεύθυνοι για την ασφάλεια web εφαρμογών θα πρέπει να συντάσσουν ένα αναλυτικό πλάνο ασφάλειας το οποίο να ικανοποιεί όλες τις απαιτήσεις ασφάλειας. Κάθε οργανισμός ηλεκτρονικού εμπορίου θα πρέπει να ακολουθεί ένα πλάνο ασφάλειας για την ορθή και ασφαλή λειτουργία του. Σύμφωνα με τους κανονισμούς της ΑΔΑΕ, οι υπεύθυνοι για την δημιουργία ενός πλάνου ασφάλειας θα πρέπει να λαμβάνουν υπόψη τα εξής:

Αναγνώριση και έλεγχος αυθεντικότητας.
Αναγνωριστικά χρηστών: Με τη βοήθεια των αναγνωριστικών εξασφαλίζεται η ταυτοποίηση κάθε χρήστη.
Επιλογή κωδικών πρόσβασης: Οι κωδικοί πρόσβασης (passwords) που υιοθετούν οι χρήστες πρέπει να έχουν αρκετό μήκος και να επιλέγονται με τέτοιο τρόπο, ώστε να είναι δύσκολο για κάποιον εισβολέα να τους μαντέψει.
Αποθήκευση κωδικών πρόσβασης: Οι κωδικοί πρόσβασης των χρηστών θα πρέπει να αποθηκεύονται σε κατάλληλη μορφή, ώστε κανείς, ακόμα και ο διαχειριστής του συστήματος να μην μπορεί να τους διαβάσει.
Συχνότητα αλλαγής κωδικών πρόσβασης: Οι κωδικοί πρόσβασης πρέπει να αλλάζουν αρκετά συχνά, ώστε να διασφαλίζεται η εμπιστευτικότητα τους.

Έλεγχος πρόσβασης.
Δικαιώματα πρόσβασης: Για κάθε νέο λογαριασμό χρήστη θα πρέπει να καθορίζονται τα δικαιώματα πρόσβασης στους πόρους του συστήματος.
Αδρανής σταθμός εργασίας: Οι σταθμοί εργασίας θα πρέπει να κλειδώνονται όταν μένουν αδρανείς για κάποιο χρονικό διάστημα, ώστε να περιοριστεί η πιθανότητα ένας μη εξουσιοδοτημένος χρήστης να αποκτήσει πρόσβαση.
Διαχείριση δικαιωμάτων: Κατάλληλος μηχανισμός επιτρέπει την πρόσβαση σε ιδιαίτερες λειτουργίες του συστήματος μόνο σε χρήστες που πρέπει να έχουν πρόσβαση σε αυτές.
Ασφάλεια του λογισμικού εφαρμογών: Η πρόσβαση στα αρχεία του λογισμικού εφαρμογών θα πρέπει να ελέγχεται με τη βοήθεια κατάλληλων προγραμμάτων.

Απόδοση ευθυνών.
Καταγραφή γεγονότων: Πρόκειται για την καταγραφή όλων των περιστατικών που

λαμβάνουν χώρα στο σύστημα κάθε χρονική στιγμή, ώστε κάθε επεισόδιο να μπορεί να διερευνηθεί και να αποδοθούν ευθύνες.
Διατήρηση των αρχείων καταγραφής γεγονότων: Θα πρέπει να διατηρείται κατάλληλο αρχείο καταγραφής γεγονότων για αρκετό χρονικό διάστημα.
Διερεύνηση επεισοδίων: Όταν κάποια επεισόδια ανιχνεύονται ή υπάρχουν υποψίες για αυτά, πρέπει να διερευνούνται σε βάθος.

Προστασία από ιούς.
Πρόληψη και αποτροπή: Θα πρέπει να ελαχιστοποιηθεί η πιθανότητα να προσβληθεί το σύστημα από ιούς οποιασδήποτε μορφής.
Ανίχνευση: Το σύστημα θα πρέπει να περιλαμβάνει μηχανισμούς περιοδικού ελέγχου για ιούς. Αντιμετώπιση: Θα πρέπει να υπάρχουν κατάλληλοι μηχανισμοί απομόνωσης και καταστροφής ιών.

Διαχείριση ασφάλειας δικτύου.
Παρακολούθηση του δικτύου: Η κατάσταση του δικτύου θα πρέπει να παρακολουθείται, ώστε να διευκολύνεται η έγκαιρη ανίχνευση των προβλημάτων.
Εμπιστευτικότητα δεδομένων στο δίκτυο: Η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω δικτύου θα πρέπει να προστατεύεται.

Έλεγχος πρόσβασης μέσω δικτύου
Απομακρυσμένη πρόσβαση σε μη ενεργές θύρες: Μόνο οι θύρες (ports) που χρησιμοποιούνται θα πρέπει να είναι ενεργές και οι υπόλοιπες πρέπει να είναι κλειδωμένες.
Firewalls: Τα δίκτυα πρέπει να προστατεύονται μέσω των φραγμάτων ασφαλείας.

Διαχείριση συστήματος.
Διαδικασίες: Δημιουργία εγγράφου στο οποίο θα καθορίζονται αναλυτικά οι διαδικασίες εκτέλεσης των σημαντικότερων εργασιών.
Έλεγχος πρόσβασης στο λογαριασμό του διαχειριστή του συστήματος: Ο λογαριασμός του διαχειριστή συστήματος είναι ο πιο προνομιούχος λογαριασμός στο σύστημα και για αυτό η χρήση του θα πρέπει να ελέγχεται.

Σχέδιο συνέχειας.
Αποκατάσταση λειτουργίας: Ο υπεύθυνος ασφάλειας θα πρέπει να καταρτίσει σχέδιο συνέχειας για περιπτώσεις αντιμετώπισης έκτακτων περιστατικών και διαδικασιών ανάνηψης. Οι υπολογιστές του συστήματος και οι υπηρεσίες δικτύου θα πρέπει να είναι διαθέσιμες όταν χρειάζονται.
Εφεδρικά αντίγραφα: Η ύπαρξη εφεδρικών αντιγράφων εξασφαλίζει τη συνεχή διαθεσιμότητα των δεδομένων.

ΜΕΡΟΣ 3ο

ΚΡΥΠΤΟΓΡΑΦΗΣΗ : ΤΟ Α ΚΑΙ ΤΟ Ω ΤΗΣ ΔΙΑΔΙΚΤΥΑΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΚΕΦΑΛΑΙΟ 5

ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Η λέξη κρυπτολογία αποτελείται από την ελληνική λέξη κρύπτο – κρυφός και την λέξη λόγος. Είναι ο τομέας που ασχολείται με την μελέτη της ασφαλούς επικοινωνίας. Ο κύριος στόχος είναι να παρέχει μηχανισμούς για 2 ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάζει την πληροφορία εκτός από τα μέλη.

5.1 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΤΗς ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η κρυπτογραφία είχε αρχικά την μορφή τέχνης που τα μυστικά της γνώριζαν λίγοι και εκλεκτοί. Η ιστορία της κρυπτογραφίας ξεκινά περίπου το 4000 π.Χ. στην αρχαία Αίγυπτο περνά στην αρχαία Ελλάδα που έχουμε αναφορές της στο ιστορικό Πολύβιο και συνεχίζεται στον Ιούλιο Καίσαρα. Ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του, με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του. Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο, όχι όμως τυχαία επιλεγμένο. Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά. Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί π.χ. 3. Δηλαδή, η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο. Θα μπορούσε το κλειδί να ήταν ο αριθμός 6, οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό. Έτσι, διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα.

Ο πίνακας αντιστοιχίσεις των γραμμάτων, έχοντας ως κλειδί το 3, φαίνεται παρακάτω:

Το γράμμα	a	b	c	d	e	f	g	h	i	j	k	v	mn	o	p	q	r	s	t	u	v	w	x	y	z
Αντικαθίσταται από το γράμμα	d	e	f	g	h	i	j	k	l	mn	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Αν, για παράδειγμα, το απλό κείμενο είναι η λέξη secret, θα προκύψει το κρυπτογράφημα wigvix. Για να το αποκρυπτογραφήσει κάποιος θα πρέπει να αντιστρέψει τη διαδικασία κρυπτογράφησης, με άλλα λόγια να αντικαταστήσει κάθε γράμμα με αυτό που βρίσκεται 3 θέσεις αριστερότερά του στο αλφάβητο. Προφανώς, δεν αρκεί να ξέρει ότι ο κατάλληλος αλγόριθμος αποκρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα αριστερά, αλλά πρέπει να γνωρίζει και πόσες θέσεις χρειάζεται να τα ολισθήσει. Πρέπει να γνωρίζει το κλειδί, που σε αυτήν την περίπτωση είναι ο αριθμός 3 .

Από την στιγμή που η κρυπτογραφία άρχισε να χρησιμοποιείται για στρατιωτικούς σκοπούς και για απόκρυψη ζωτικής σημασίας πληροφοριών, έπαψε να είναι απόκρυφη τέχνη και έτυχε της μελέτης τόσο αυτών που ήθελαν να αποκρύψουν τα μυστικά τους όσο και από αυτούς που ήθελαν να βρουν τρόπο να αποκαλύψουν τα μυστικά των αντιπάλων τους. Έτσι η κρυπτογραφία πέρασε στο πεδίο της επιστήμης. Κρυπτογράφοι και κρυπταναλυτές επιδόθηκαν σε έναν ανελέητο συναγωνισμό. Κάθε πρόοδος της κρυπτογραφίας συνοδευόταν από μια αντίστοιχη πρόοδο της κρυπτανάλυσης. Η κρυπτογραφία έγινε χρήσιμο εργαλείο στα χέρια του στρατού των διπλωματών και του κράτους με σκοπό την διαφύλαξη εθνικών μυστικών και στρατηγικών. Όσο πιο πολύτιμα τα μυστικά τόσο πιο μεγάλη αξία αποκτούσε η ασφαλής φύλαξή τους. Στον 20ό αιώνα τα παραδείγματα εκτεταμένης χρήσης κρυπτογραφικών τεχνικών είναι πολλά .

Την περίοδο της ποτοαπαγόρευσης στην Αμερική (δεκαετία του 20-30) το νεοσύστατο τότε σώμα FBI χρησιμοποίησε τεχνικές κρυπτογραφίας για να αποκρύπτει από τη μαφία τους τόπους παράδοσης μεγάλων φορτίων ποτών.

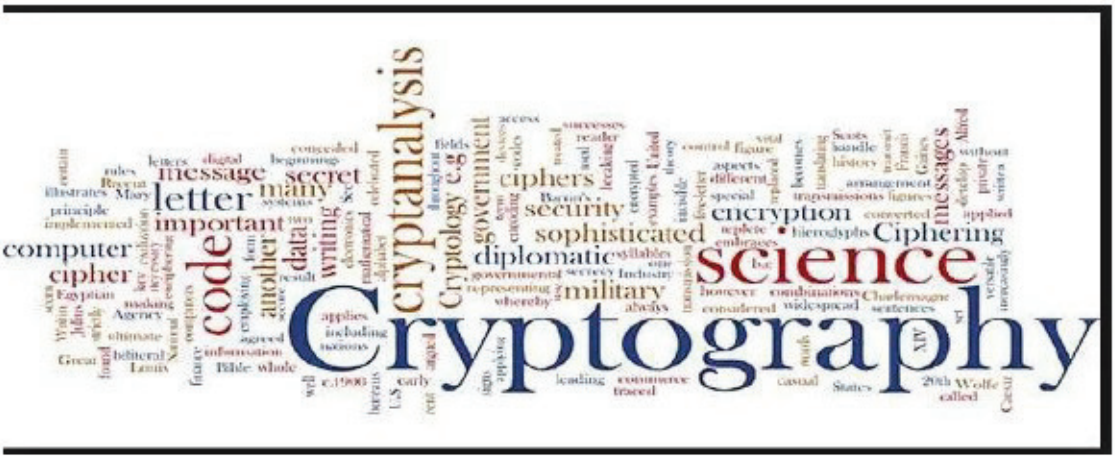
Δεν θα ήταν υπερβολή να πούμε ότι η έκβαση του δευτέρου Παγκοσμίου Πολέμου κρίθηκε υπέρ των συμμάχων εξαιτίας της ικανότητας τους να αποκρυπτογραφούν τα γερμανικά μηνύματα και της ανικανότητας των Γερμανών να πράξουν κάτι ανάλογο με τα συμμαχικά μηνύματα. Είναι γνωστή άλλωστε η ιστορία της μηχανής ENIGMA που χρησιμοποίησαν οι Άγγλοι για να αποκρυπτογραφούν τα μηνύματα του Γερμανικού επιτελείου προς τις αγέλες των υποβρυχίων τους στη Μεσόγειο αλλά και τον Ατλαντικό ωκεανό.

Από την δεκαετία του 60 και μετά η κρυπτογραφία γνώρισε μεγάλη ανάπτυξη λόγω της ραγδαίας ανάπτυξης των υπολογιστών, αλλά και των τηλεπικοινωνιών. Έτσι λοιπόν, υπήρξε η ανάγκη για προστασία δεδομένων σε ψηφιακή μορφή. Αρχίζοντας με την εργασία του Feistel στην IBM στις αρχές της δεκαετίας του '70 και καταλήγοντας το 1977 με την υιοθέτηση του Αμερικανικού ομοσπονδιακού προτύπου για την επεξεργασία των πληροφοριών την κρυπτογράφηση των μη-διαβαθμισμένων πληροφοριών, τον αλγόριθμο DES. Παραμένει μέχρι σήμερα το τυποποιημένο μέσο για την ασφάλεια του ηλεκτρονικού εμπορίου σε πολλά οικονομικά ιδρύματα σε όλο τον κόσμο.

Η πιο εντυπωσιακή ανάπτυξη στην ιστορία της κρυπτογραφίας ήρθε το 1976 όταν ο Diffie και ο Hellman δημοσίευσαν το “New directions in cryptography”. Αυτή η επιστημονική δημοσίευση εισήγαγε την επαναστατική έννοια τής κρυπτογραφίας δημοσίου κλειδιού. Παρόλο που οι συγγραφείς δεν έκαναν πρακτική εφαρμογή του σχήματος που πρότειναν, η αρχή είχε γίνει και το θέμα έτυχε μεγάλου ενδιαφέροντος από την κρυπτογραφική κοινότητα.
Το 1978 οι Rivest, Shamir και Adleman ανακάλυψαν την πρώτη πρακτική εφαρμογή του προταθέντος σχήματος. Ήταν το λεγόμενο σχήμα RSA και βασιζόταν σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, αυτό της δυσκολίας παραγοντοποίησης μεγάλων ακεραίων. Όπως ήταν φυσικό οι κρυπταναλυτές σήκωσαν τα μανίκια και άρχισαν να ψάχνουν πιο αποτελεσματικούς τρόπους παραγοντοποίησης. Παρά τις μεγάλες προόδους τους κυρίως την δεκαετία του 80 το RSA παρέμεινε ακόμα

ασφαλές! Μια από τις σημαντικότερες προσφορές της κρυπτογραφίας δημοσίου κλειδιού ήταν και η ψηφιακή υπογραφή.

5.2 ΚΡΥΠΤΟΛΟΓΙΑ



Η Κρυπτολογία χωρίζεται σε 2 επιμέρους ενότητες:

1. Κρυπτογραφία: η επιστήμη που ασχολείται με τους μαθηματικούς μετασχηματισμούς για την εξασφάλιση της ασφάλειας της πληροφορίας

2. Κρυπτανάλυση: η επιστήμη που ασχολείται με την ανάλυση και την διάσπαση των Κρυπτοσυστημάτων

Η κρυπτογραφία παρέχει 4 βασικές λειτουργίες (αντικειμενικοί σκοποί):

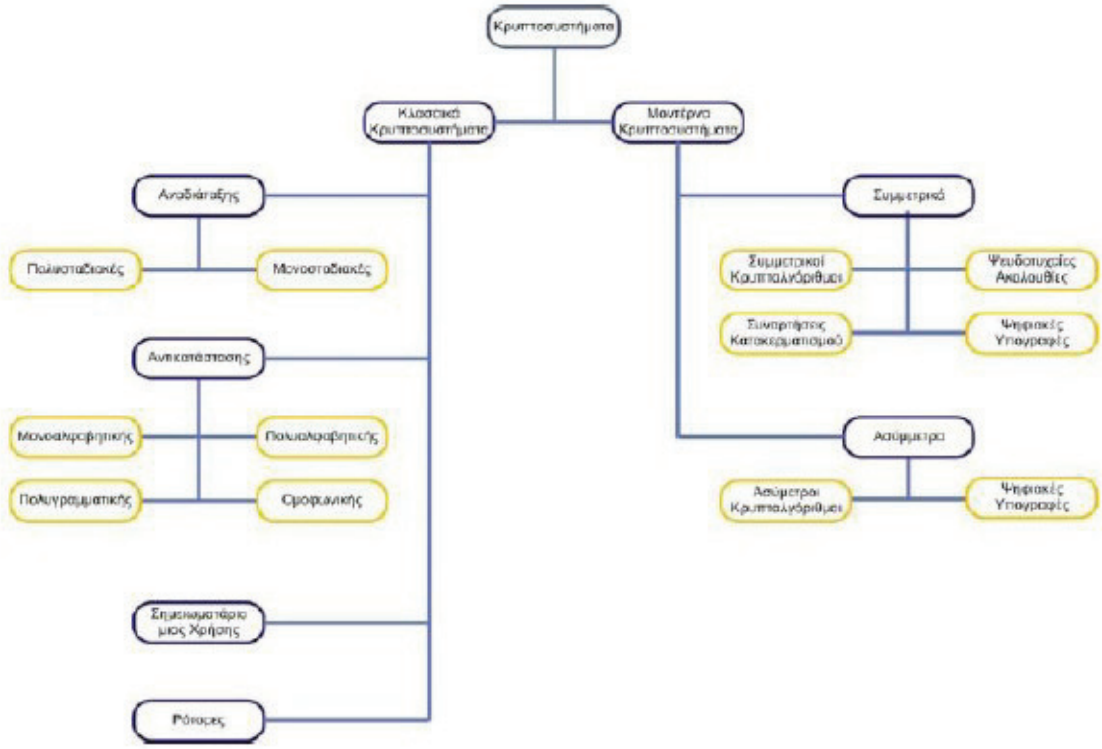
- Εμπιστευτικότητα: Η πληροφορία προς μετάδοση είναι προσβάσιμη μόνο στα εξουσιοδοτημένα μέλη. Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο.

- Ακεραιότητα: Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης.

- Μη αποποίηση: Ο αποστολέας ή ο παραλήπτης της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης ή της δημιουργίας της.

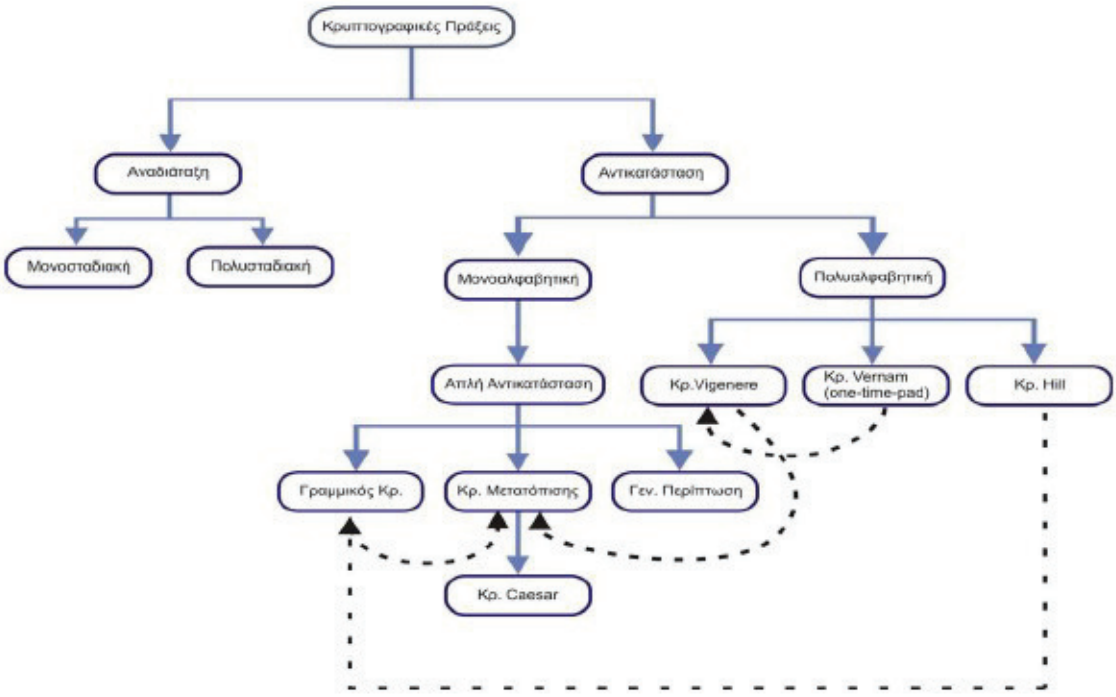
- Αυθεντικοποίηση: Οι αποστολέας και παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι πλαστές.

Η κρυπτανάλυση ασχολείται με τα κρυπτοσυστήματα που χωρίζονται σε 2 μεγάλες κατηγορίες τα οποία είναι τα εξής (Σχήμα 5.1):
α) τα Κλασσικά Κρυπτοσυστήματα
β) τα Μοντέρνα Κρυπτοσυστήματα



5.3 ΤΑ ΚΛΑΣΙΚΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

Τα Κλασσικά Κρυπτοσυστήματα χωρίζονται σε 2 κατηγορίες οι οποίες είναι τα εξής (Σχήμα 5.2):
Ι. αναδιάταξη (α. Πολυσταδιακές και β. Μονοσταδιακές)
ΙΙ.αντικατάσταση (α. Μονοαλφαβητικής, β. Πολυαλφαβητικής, γ. Πολυγραμματικής, δ. Ομοφωνικής)



5.3.1 ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΑΝΑΔΙΑΤΑΞΗΣ

Τα κρυπτογραφήματα αναδιάταξης διατηρούν τη σειρά των συμβόλων του καθαρού κειμένου αλλά παραποιούν τα ίδια τα σύμβολα. Τα κρυπτογραφήματα αναδιάταξης αλλάζουν τη σειρά των συμβόλων, χωρίς να τα παραποιούν.
Η κρυπτογράφηση γίνεται ως εξής:
Αρχικά τοποθετούμε το καθαρό κείμενο σε έναν πίνακα. Από κάθε γραμμή αντλούμε τα γράμματα που απαρτίζουν το κρυπτογραφημένο κείμενο με διαφορετική σειρά που γράφεται στο καθαρό κείμενο. Με τον τρόπο αυτό καταφέρνουμε να αναδιατάξουμε τα γράμματα του καθαρού κειμένου για τη παραγωγή του κρυπτογραφήματος. Το κλειδί σε αυτή τη περίπτωση είναι η σειρά με την οποία λαμβάνουμε τα κρυπτογραφημένα σύμβολα και ο αριθμός των στηλών του πίνακα. Ένας τρόπος με τον οποίο μπορούμε να καθορίσουμε το κλειδί είναι χρησιμοποιώντας κωδικές λέξεις ή φράσεις των οποίων τα γράμματα καθορίζουν τη σειρά ανάλογα με τη θέση τους στην αλφάβητο.
Η παραβίαση και αυτού του κρυπτογραφήματος γίνεται με χρήση των στατιστικών ιδιοτήτων της χρησιμοποιούμενης γλώσσας και με εύρεση του μέγεθους του κλειδιού.

5.3.2 ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ

Σε ένα κρυπτογράφημα αντικατάστασης κάθε γράμμα ή ομάδα γραμμάτων αντικαθίσταται από ένα άλλο γράμμα ή ομάδα γραμμάτων. Το παλαιότερο γνωστό κρυπτογράφημα τέτοιου είδους είναι το κρυπτογράφημα Καίσαρα. Σύμφωνα μ' αυτή τη μέθοδο το αλφάβητο του κρυπτογραφημένου κειμένου ολισθαίνει κατά 3 γράμματα. Γενικότερα, μπορεί να γίνει ολίσθηση κατά k γράμματα.

Στη περίπτωση αυτή το k είναι το κλειδί του κρυπτογραφήματος. Μπορούμε να ορίσουμε τη μέθοδο κρυπτογράφησης αντικαθιστώντας κάθε γράμμα με ένα άλλο γράμμα χρησιμοποιώντας έναν οποιοδήποτε τυχαίο αλγόριθμο.
Στη περίπτωση αυτή η μέθοδος ονομάζεται μονοαλφαβητική αντικατάσταση και το κλειδί είναι η ακολουθία των γραμμάτων που αντιστοιχεί σε όλη την αλφάβητο. Ενώ η παραπάνω μέθοδος φαίνεται εκ πρώτης όψεως ασφαλής, εντούτοις, χρησιμοποιώντας τις στατιστικές ιδιότητας μιας γλώσσας μπορούμε εύκολα να σπάσουμε τον κώδικα.

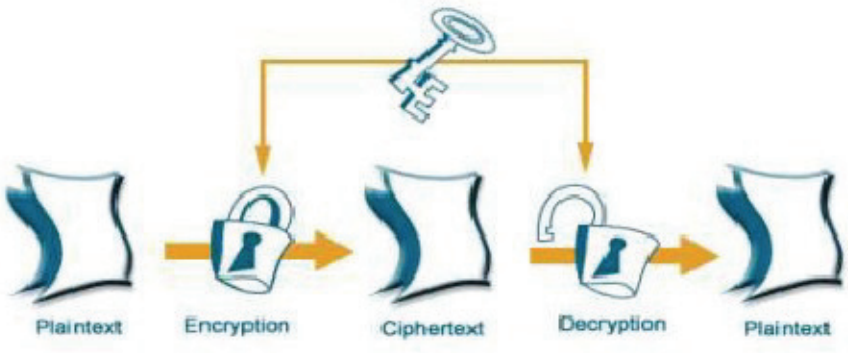
5.4 ΤΑ ΜΟΝΤΕΡΝΑ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΑ

Τα Μοντέρνα Κρυπτοσυστήματα χωρίζονται σε 2 κατηγορίες οι οποίες είναι τα εξής:
I. Συμμετρικά Κρυπτοσυστήματα
II. Ασύμμετρα Κρυπτοσυστήματα

5.4.1 ΣΥΜΜΕΤΡΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Εισαγωγή για την Συμμετρική Κρυπτογραφία

Χρησιμοποιεί η συμμετρική κρυπτογραφία το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση (Σχήμα 5.3). Αρχικά, το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα μέρη και, άρα, απαιτείται ασφαλές μέσο για τη μετάδοσή του, για παράδειγμα μία προσωπική συνάντηση κατά την οποία θα συμφωνηθεί το κλειδί που θα χρησιμοποιείται. Αν κάτι τέτοιο δεν είναι εφικτό, η συμμετρική κρυπτογραφία είναι αναποτελεσματική.



Στη συμμετρική Κρυπτογραφία υπάρχουν αρκετοί αλγόριθμοι, ο πιο γνωστός είναι ο Data Encryption Standard (DES), ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Η.Π.Α. ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών.

Τα συστήματα συμμετρικής κρυπτογραφίας προϋποθέτουν την ύπαρξη ενός ασφαλούς καναλιού για την ανταλλαγή των μυστικών κλειδιών δηλ. αυτά που επιτρέπουν την ασφαλή ανταλλαγή κλειδιών μέσα από δημόσια δίκτυα έχουν αναπτυχθεί και χρησιμοποιούνται, με περισσότερο διαδεδομένο το σύστημα Kerberos που έχει αναπτυχθεί στο MIT.

Κανόνες Συμμετρικής Κρυπτογραφίας

Η συμβατική κρυπτογραφία (conventional cryptography) αναφερόμενη ως συμμετρική κρυπτογραφία (symmetric cryptography) ή κρυπτογραφία μυστικού κλειδιού (secret key cryptography) αποτελούσε το μοναδικό τύπο κρυπτογράφησης δημόσιου κλειδιού. Ένα σχήμα συμβατικής κρυπτογραφίας αποτελείται από πέντε επιμέρους οντότητες όπως φαίνεται στο παραπάνω σχήμα (Σχήμα 5.3):

- Αρχικό κείμενο (plaintext): Αποτελείται από τα αρχικά μηνύματα ή δεδομένα που εισάγονται στον αλγόριθμο κρυπτογράφησης.

- Αλγόριθμος κρυπτογράφησης (encryption algorithm): Πραγματοποιεί τους απαραίτητους μετασχηματισμούς του αρχικού κειμένου για την επίτευξη κρυπτογράφησης ενός μηνύματος.

- Μυστικό κλειδί (secret key): Αποτελεί το μυστικό κλειδί, το οποίο εισάγεται επίσης στον αλγόριθμο κρυπτογράφησης. Οι ακριβείς αντικαταστάσεις και τα αποτελέσματα των μετασχηματισμών που επιτελούνται από τον αλγόριθμο εξαρτώνται από αυτό το μυστικό κλειδί.

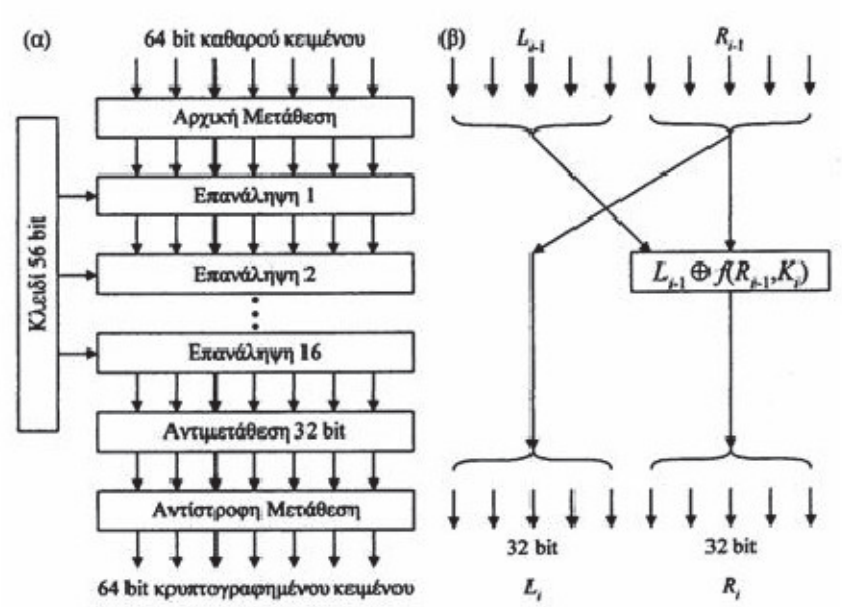
- Κρυπτογράφημα ή κρυπτογραφημένο μήνυμα (chiphertext): Αυτό είναι το μετασχηματισμένο μήνυμα του κειμένου που παράγεται ως έξοδος από τον αλγόριθμο κρυπτογράφησης. Το κρυπτογράφημα αυτό εξαρτάται τόσο από το αρχικό μήνυμα όσο και από το μυστικό κλειδί, συνεπώς δοθέντος ενός μηνύματος διαφορετικά κλειδιά παράγουν διαφορετικά κρυπτογραφήματα.

- Αλγόριθμος αποκρυπτογράφησης (decryption algorithm): Αυτός είναι απαραίτητα ο αλγόριθμος κρυπτογράφησης εκτελεσμένος αντίστροφα την διαδικασία, δηλαδή λαμβάνει το κρυπτογραφημένο κείμενο και το ίδιο μυστικό κλειδί που χρησιμοποιήθηκε στη διαδικασία της κρυπτογράφησης και παράγει το αρχικό κείμενο.

Οι αλγόριθμοι Κρυπτογράφησης

Οι περισσότερο συχνά χρησιμοποιημένοι συμβατικοί αλγόριθμοι κρυπτογράφησης είναι οι κρυπτογραφήσεις τμημάτων. Μια κρυπτογράφηση τμήματος επεξεργάζεται την καθαρή είσοδο σε καθορισμένου μεγέθους τμήματα και παράγει ένα τμήμα κρυπτογραφημένου κειμένου ίσου μεγέθους με κάθε τμήμα καθαρού κειμένου. Παρακάτω θα δούμε τους πιο σημαντικούς αλγόριθμους

Γενικά για τον αλγόριθμο Data Encryption Standard



Το πρότυπο κρυπτογράφησης δεδομένων Data Encryption Standard (DES) είναι ένας αλγόριθμος συμμετρικής κρυπτογράφησης (είναι μια μέθοδος κρυπτογράφησης για τις πληροφορίες) που επιλέχθηκε επίσημα για την χρήση του από τον οργανισμό Federal Information Processing Standard (FIPS) στις Ηνωμένες Πολιτείες το 1976, και το οποίο στη συνέχεια χρησιμοποιήθηκε ευρέως διεθνώς. Ο αλγόριθμος αρχικά αμφισβητήθηκε, όσον αφορά σε απόρρητες πληροφορίες του σχεδιασμού στοιχείων, το σχετικά μικρό μήκος του κλειδιού (short key length) και την έμμεση ανάμειξη της Υπηρεσίας Εθνικής Ασφάλειας (National Security Agency NSA). Ο αλγόριθμος DES κατά συνέπεια έγινε αντικείμενο έντονης ακαδημαϊκής έρευνας, και παρακίνησε τη σύγχρονη κατανόηση του κρυπτογραφήματος (block ciphers) και της κρυπτολογικής ανάλυσής του.
Ο αλγόριθμος DES θεωρείται σήμερα επισφαλής για πολλές εφαρμογές. Αυτό οφείλεται κυρίως στο γεγονός ότι το μέγεθος του κλειδιού (56 bit) είναι πάρα πολύ μικρό. Κλειδιά του αλγορίθμου DES έχουν αποκωδικοποιηθεί σε λιγότερο από 24 ώρες. Υπάρχουν επίσης μερικά αναλυτικά αποτελέσματα τα οποία αποδεικνύουν θεωρητικές αδυναμίες του κρυπτογραφήματος, οι οποίες ωστόσο στην πράξη δεν μπορούν να αποδειχτούν. Ο αλγόριθμος πιστεύεται ότι στην πράξη είναι ασφαλής υπό την μορφή τριπλού DES (Triple DES), αν και υπάρχουν θεωρητικές αντιρρήσεις. Τα τελευταία χρόνια, η κρυπτογραφία έχει διαδεχθεί από προηγμένα πρότυπα κρυπτογράφησης, το πρότυπο Advanced Encryption Standard (AES).
Σε κάποια έγγραφα τεκμηρίωσης, γίνεται διάκριση ανάμεσα στο DES ως πρότυπο και στον αλγόριθμο που είναι γνωστός ως DEA (Data Encryption Algorithm – Αλγόριθμος Κρυπτογράφησης Δεδομένων).

Η ιστορία του αλγορίθμου Des

Ο αλγόριθμος DES δημιουργήθηκε στης αρχές της δεκαετίας του '70. Αργότερα το 1972, με την ολοκλήρωση μελέτης για τις ανάγκες ασφάλειας των υπολογιστών της Αμερικανικής Κυβέρνησης, το σώμα Αμερικανικών Προτύπων NBS (National Bureau of Standards) προσδιόρισε την ανάγκη ύπαρξης ενός κοινού πρότυπου για την κρυπτογράφηση των μη απόρρητων και ευαίσθητων πληροφοριών για όλη την κυβέρνηση. Έτσι, στις 15 Μαΐου 1973, μετά από σύσκεψη με την NSA, το NBS ζήτησε τις προτάσεις για ένα πρότυπο κρυπτογράφησης που θα ικανοποιούσε τα αυστηρά κριτήρια σχεδιασμού του. Εντούτοις, καμία από τις υποβαλλόμενες προτάσεις δεν αποδείχθηκε κατάλληλη. Ένα δεύτερο αίτημα εκδόθηκε στις 27 Αυγούστου 1974. Αυτή τη φορά, η IBM υπέβαλε μία πρόταση που κρίθηκε αποδεκτή, και ένα πρότυπο κρυπτογράφησης αναπτύχθηκε κατά την διάρκεια της περιόδου 1973-1974 βασισμένο σε έναν προηγούμενο αλγόριθμο, το πρότυπο Horst Feistel's Lucifer. Η ομάδα της IBM για τον σχεδιασμό και την ανάλυση του κρυπτογραφήματος περιλάμβανε τους Feistel, Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith, και Bryant Tuckerman.

Ο αλγόριθμος ως πρότυπο

Παρά τις κριτικές, το DES εγκρίθηκε ως ομοσπονδιακά πρότυπο το Νοεμβρίου του 1976, και δημοσιεύθηκε στις 15 Ιανουαρίου 1977 ως FIPS PUB 46, κατάλληλο για χρήση σε όλα στα μη απόρρητα δεδομένα. Επιβεβαιώθηκε στη συνέχεια ως πρότυπο το 1983, το 1988 (που αναθεωρήθηκε ως FIPS-46-1), το 1993 (FIPS-46-2), και πάλι το 1998 (FIPS-46-3), τα τελευταία που ορίζουν «τριπλό DES».

Στις 26 Μαΐου 2002, το DES εκτοπίστηκε τελικά από το AES, το προηγμένο πρότυπο κρυπτογράφησης, μετά από έναν δημόσιο ανταγωνισμό. Ακόμη και το 2004, ωστόσο, το DES παραμένει σε διαδεδομένη χρήση. Στις 19 Μαΐου 2005, το FIPS 46-3 αποσύρθηκε επίσημα, αλλά η NIST έχει εγκρίνει το τριπλό DES έως το 2030 για τις ευαίσθητες κυβερνητικές πληροφορίες.

Μια άλλη θεωρητική επίθεση, η γραμμική κρυπτολογική ανάλυση, δημοσιεύθηκε το 1994, αλλά ήταν μια σφοδρή επίθεση το 1998 που κατέδειξε ότι το DES θα μπορούσε να πληγεί πρακτικά, και έδωσε έμφαση στην ανάγκη για έναν αλγόριθμο αντικατάστασης.

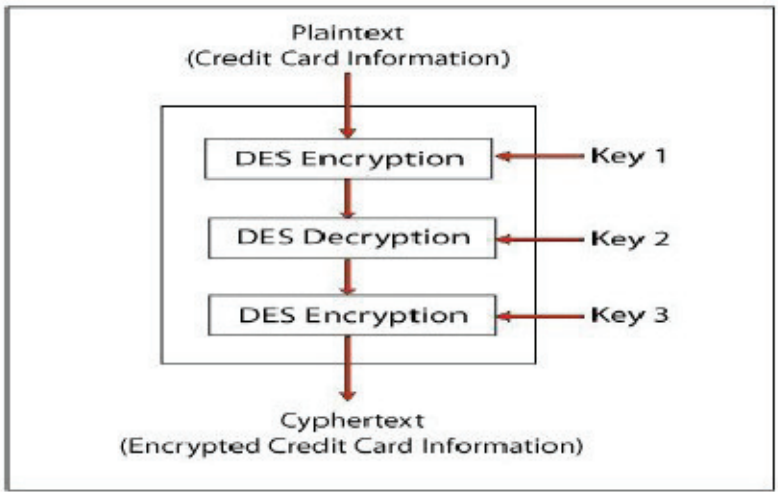
Η δημιουργία του DES θεωρείται καταλυτικής σημασίας για την ακαδημαϊκή μελέτη του συστήματος κρυπτογραφίας, ιδιαίτερα όσον αφορά στις μεθόδους για την αποκρυπτογράφηση το κρυπτογραφικών block.

Αλγόριθμοι αντικατάστασης

Οι ανησυχίες για την ασφάλεια και τη σχετικά αργή λειτουργία του DES στο λογισμικό παρακίνησαν τους ερευνητές να προτείνουν ποικίλα εναλλακτικά σχέδια για block cipher, τα οποία άρχισαν να εμφανίζονται προς το τέλος της δεκαετίας του '80 και τις αρχές τις δεκαετίας του '90. Τα περισσότερα από αυτά τα σχέδια κράτησαν ως μέγεθος του DES τα 64-bit, και θα μπορούσαν να ενεργήσουν ως αντικατάσταση,

αν και χρησιμοποίησαν τυπικά ένα κλειδί 64-bit ή 124-bit. Στην USSR εισήχθη ο αλγόριθμος GOST 28147-89, με μέγεθος block 64-bit και ένα κλειδί 256-bit, το οποίο χρησιμοποιήθηκε επίσης στη Ρωσία αργότερα.
Το ίδιο το DES μπορεί να προσαρμοστεί και να επαναχρησιμοποιηθεί σε ένα ασφαλέστερο σχέδιο. Πολλοί πρώην χρήστες DES χρησιμοποιούν τώρα Triple DES (TDES) που περιγράφηκε και αναλύθηκε από έναν από τους σχεδιαστές του DES. Περιλαμβάνει την εφαρμογή του DES τρεις φορές με δύο (2TDES) ή τρία (3TDES) διαφορετικά κλειδιά. Το TDES θεωρείται επαρκώς ασφαλές, αν και είναι αρκετά αργό. Μια λιγότερο ακριβή εναλλακτική λύση είναι το DES-X, το οποίο αυξάνει το μέγεθος του κλειδιού από XORing το πρόσθετο κλειδί υλικό πριν και μετά από DES. Το GDES ήταν μια εναλλακτική του DES μεταβλητή που προτάθηκε ως τρόπος να επιταχυνθεί η κρυπτογράφηση, αλλά αποδείχθηκε ευαίσθητο στη διαφορική κρυπτολογική ανάλυση.
Το 2001, μετά από έναν διεθνή διαγωνισμό, η NIST επέλεξε ένα νέο κρυπτογραφικό πρότυπο: τα πρότυπα AES, ως αντικατάσταση. Ο αλγόριθμος που επιλέχτηκε ως AES υποβλήθηκε από τους σχεδιαστές του με το όνομα Rijndael. Οι άλλες συμμέτοχες στην NIST επικράτησε το AES συμπεριλαμβάνεται επίσης και οι αλγόριθμοι RC6, Serpent, MARS, και Towfish.
Το DES είναι ένας αρχετυπικός κρυπτογραφικό block - ένας αλγόριθμος που παίρνει μια καθορισμένου μήκους σειρά αρχικό κείμενο (plaintext) bits και την μετασχηματίζει μέσω μιας σειράς περίπλοκων διαδικασιών σε ένα άλλο κρυπτογραφημένο μήνυμα (ciphertext) του ίδιου μήκους. Στην περίπτωση του DES, το μέγεθος του block είναι 64 bit. Το DES χρησιμοποιεί επίσης ένα κλειδί για να προσαρμόσει το μετασχηματισμό, έτσι ώστε η αποκρυπτογράφηση να μπορεί να εκτελεσθεί μόνο από εκείνους που ξέρουν το ιδιαίτερο κλειδί που χρησιμοποιείται για να κρυπτογραφηθεί. Το κλειδί αποτελείται φαινομενικά από 64 bit. Ωστόσο, μόνο 56 bit από αυτά χρησιμοποιούνται πραγματικά από τον αλγόριθμο. Οκτώ bit χρησιμοποιούνται απλώς για τον έλεγχο της ισότητας, και απορρίπτονται μετά. Ως εκ τούτου το αποτελεσματικό βασικό μήκος είναι 56 bit, και αναφέρεται συνήθως υπό αυτήν τη μορφή.
Όπως άλλα block ciphers, το DES από μόνο του δεν είναι ένας ασφαλής τρόπος κρυπτογράφησης αλλά πρέπει αντ' αυτού να χρησιμοποιηθεί σε έναν τρόπο λειτουργίας. Το Fips-81 διευκρινίζουν διάφορους τρόπους για τη χρήση με DES.

Ο αλγόριθμος Triple Data Encryption Standard (TDES)



Ο αλγόριθμος (TDES) ονομάζεται Triple Data Encryption Standard σε συντομογραφία TDES ή TDEA ή συνηθέστερα 3DES προτάθηκε αρχικά από τον W. Tuchman. Το 1985 ο αλγόριθμος 3DES, για πρώτη φορά για χρήση σε οικονομικές εφαρμογές προτυποποιήθηκε στο πρότυπο ANSI X9.17. Το 1999, με τη δημοσίευση του ως FIPS PUB 46-3, το TDES ενσωματώθηκε ως τμήμα της προτυποποίησης κρυπτογράφησης δεδομένων DES. αλγόριθμος (TDES) ονομάζεται Triple Data Encryption Standard σε συντομογραφία TDES ή TDEA .

Ο αλγόριθμος TDES ακολούθησε το πρότυπο 2DES , ο οποίος δεν αξιοποιήθηκε ευρέως αφού θεωρήθηκε ευάλωτος στις κρυπταναλυτικές επιθέσεις τύπου ενδιάμεσου (man-in-the-middle attack). Το TDES χρησιμοποιεί τρία κλειδιά και τρεις εκτελέσεις του αλγορίθμου DES. Ο αλγόριθμος ακολουθεί τη διαδοχή: κρυπτογράφηση αποκρυπτογράφηση, κρυπτογράφηση (EDE -encryption - decryption -ecryption):

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

όπου:

που: C = κρυπτογράφημα
P = αρχικό κείμενο

$E_K[X]$ = κρυπτογράφηση

$D_K[Y]$ = αποκρυπτογράφηση του X χρησιμοποιώντας κλειδί K.

Η αποκρυπτογράφηση ακολουθεί ακριβώς την ίδια διαδικασία με τα κλειδιά σε αντίστροφη χρήση

$$P = D_{K1}[E_{K2}[D_{K3}[C]]]$$

Δεν υπάρχει κρυπτογραφική σημασία στη χρήση της αποκρυπτογράφησης για δεύτερο στάδιο. Το μοναδικό πλεονέκτημα είναι ότι επιτρέπει στους χρήστες του

τριπλού DES να αποκρυπτογραφούν δεδομένα από τους χρήστες του απλού DES:

$$C=E_{K1}[D_{K1}[E_{K1}[P]]]=EK1[P]$$

Με τρία διαφορετικ κλειδιά το πρότυπο TDES, διαθέτει ένα ουσιαστικό μήκους κλειδιού των 168-bit. Στα πλαίσια του FIPS 46-3 επιτρέπεται, επίσης τη χρήση δύο κλειδιών με KI = K3. Το γεγονός αυτό εξασφαλίζει ένα μήκος κλειδιού 112-bit. Το FIPS 46-3 περιλαμβάνει τις ακόλουθες οδηγίες για το TDES:

- Το TDES αποτελεί τον εγκεκριμένο από το FIPS επιλεγμένο συμβατικό αλγόριθμο κρυπτογράφησης

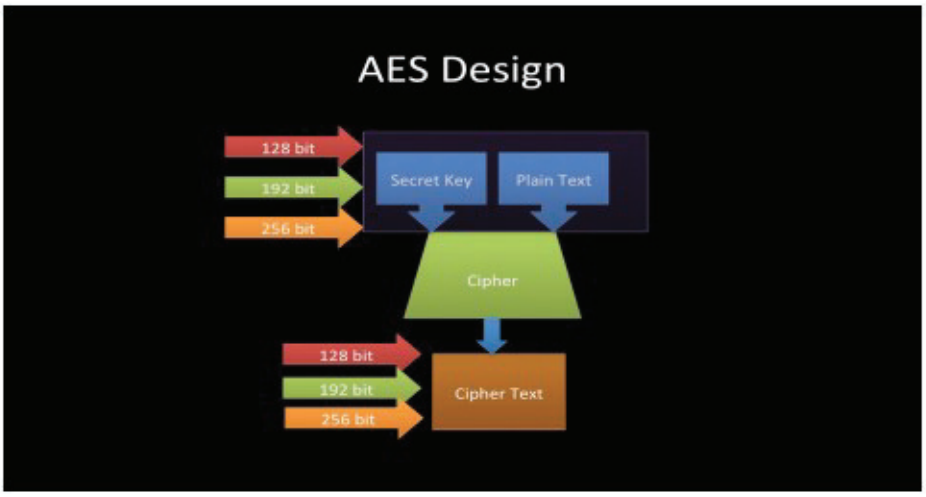
- Ο αρχικός DES, χρησιμοποιεί ένα μοναδικό κλειδί των 56-bit, επιτρέπεται κάτω από το πρότυπο μονό για κληροδοτούμενα συστήματα. Τα νέα συστήματα, όμως, πρέπει να υποστηρίζουν το TDES.

- Οι κυβερνητικοί οργανισμοί των ΗΠΑ χρησιμοποιούν τον αλγόριθμο DES για κληροδοτούμενα συστήματα ενθαρρύνονται για τη μετάβαση σε TDES.

- Είναι αναμενόμενο ότι το TDES και το Advanced Encryption Standard – AES θα συνυπάρξουν ως FIPS εγκεκριμένοι αλγόριθμοι, επιτρέποντας την σταδιακή μετάβαση στο AES.

Επιπλέον ο αλγόριθμος TDES έχει μήκος κλειδιού 168-bit και οι επιθέσεις του εξαντλητικής αναζήτησης είναι πρακτικά ατελέσφορες. Συνεπώς ο TDES αναμένεται ότι θα αξιοποιείται ολοένα και περισσότερο τα επόμενα χρόνια, μέχρι την ολοκληρωτική μετάβαση στις επερχόμενες υλοποιήσεις του AES.

Advanced Encryption Standard – AES

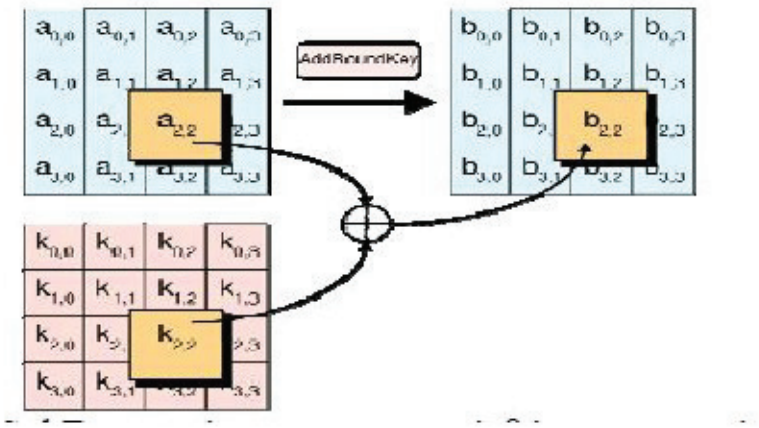


Στην κρυπτογραφία, το προηγμένο πρότυπο κρυπτογράφησης Advanced

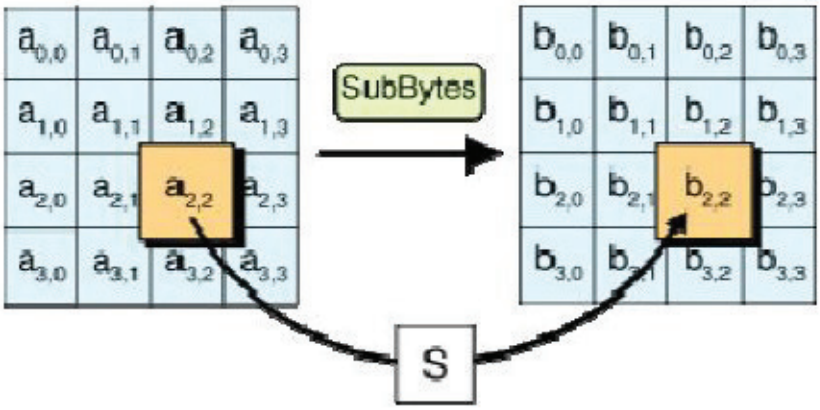
Encryption Standard (AES), επίσης γνωστό ως Rijndael, είναι ένα block cipher που έχει υιοθετηθεί ως πρότυπο κρυπτογράφησης από την Αμερικανική Κυβέρνηση. Έχει αναλυθεί εκτενώς και χρησιμοποιείται τώρα ευρέως παγκοσμίως όπως συνέβη με τον προκάτοχό του, τα πρότυπα κρυπτογράφησης δεδομένων Data Encryption Standard (DES). Ο αλγόριθμος AES αναγγέλθηκε από το εθνικό ίδρυμα προτύπων και τεχνολογίας (NIST) ως Αμερικανικό FIPS PUB 197 (FIPS 197) στις 26 Νοεμβρίου 2001 μετά από μια πενταετή διαδικασία τυποποίησης. Έγινε αποτελεσματικό ως προτύπο στις 26 Μαΐου 2002. Από το 2006, ο αλγόριθμος AES είναι ένας από τους δημοφιλέστερους αλγορίθμους που χρησιμοποιούνται στο συμμετρικό σύστημα της κρυπτογραφίας. Η κρυπτογραφία αναπτύχθηκε από δύο βέλγους κρυπτογράφους (cryptographers), από τον Joan Daemen και Vincent Rijmen, και υποβλήθηκε στην διαδικασία επιλογής του AES με το όνομα «Rijndael», ένας συνδυασμός των ονομάτων των εφευρετών. (Rijndael προφέρεται (IPA), το οποίο ηχεί σχεδόν όπως τη "Rhine doll". Περιγραφή του αλγορίθμου AES

Ο αλγόριθμος AES λειτουργεί σε μια 4×4 γραμμή ψηφιολέξεων (bytes), χρησιμοποιώντας κατάλληλη συνθήκη (οι εκδόσεις Rijndael έχουν έναμεγαλύτερο block μέγεθος τις πρόσθετες στήλες συνθηκών). την κρυπτογράφηση, κάθεκύκλος του αλγορίθμου AES (εκτός από τον τελευταίο κύκλο) αποτελείται από τέσσερα στάδια:

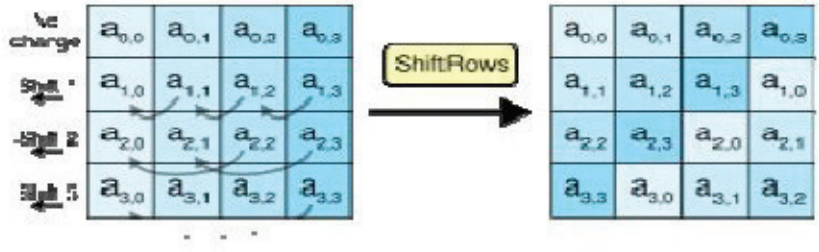
- Add Round key κάθε ψηφιολέξη(byte) της συνθήκης συνδυάζεται με το στρογγυλό κλειδί; Κάθε στρογγυλό κλειδί προέρχεται από το κρυπτογραφικό κλειδί χρησιμοποιώντας ένα κλειδί δρομολόγησης όπως βλέπουμε στο παρακάτω σχήμα.



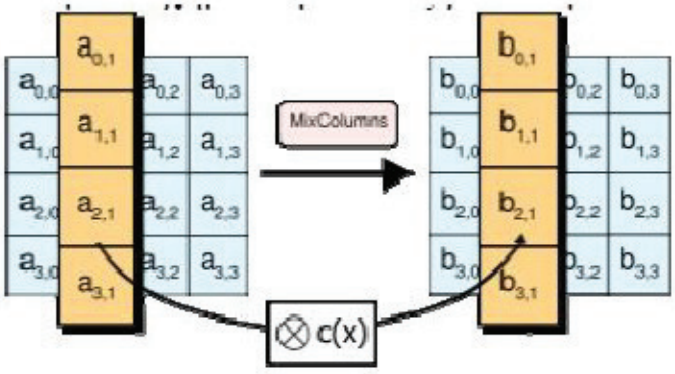
- SubBytes - ένα μη γραμμικό βήμα αντικατάστασης όπου κάθε ψηφιολέξη αντικαθίσταται με άλλη σύμφωνα με έναν πρόγραμμα κλειδιών όπως βλέπουμε στο παρακάτω σχήμα.



⊣ ShiftRows - ένα βήμα αντικατάστασης-μετάθεσης όπου κάθε γραμμή τωνψηφίωντης συνθήκης μετατοπίζεται κυκλικά ορισμένα βήματα όπως βλέπουμε στοπαρακάτω σχήμα.



⊣ MixColumns – η αντικατάσταση λειτουργεί όπως λειτουργεί στις στήλες της συνθήκης, που συνδυάζει τις τέσσερις ψηφιολέξεις (byte) σε κάθε στήλη σχήμα.



Ο τελικός κύκλος αντικαθιστά το στάδιο MixColumns με μια άλλη περίπτωση στην χρονική περίοδο το AddRoundKey.

Ο αλγόριθμος Blowfish

Ο Blowfish είναι ένας block cipher που κατασκευάστηκε από τον από τον επιφανή κρυπτογράφο B.Schneier και καθιερώθηκε ως μία από τις δημοφιλέστερες εναλλακτικές λύσεις του DES. Είναι ένας Feistel cipher με μέγεθος block 64 bits και χαρακτηριστικό γνώρισμα του Blowfish αποτελεί το μήκος κλειδιού, το οποίο είναι μεταβλητό, μπορεί να λάβει τιμές έως 448-bit, αν και πρακτικά χρησιμοποιούνται κλειδιά των 128-bit. Ο Blowfish χρησιμοποιεί 16 γύρους. Όλες οι διεργασίες βασίζονται σε X-OR πράξεις και προσθέσεις λέξεων των 32 bits. Από το κλειδί παράγεται πίνακας με τα subkeys που χρησιμοποιούνται σε κάθε γύρο επανάληψης της κρυπτογράφησης. Έχει σχεδιασθεί για 32-bit μηχανές και είναι σημαντικά ταχύτερος από τον DES. Παρ' όλες τις αδυναμίες που έχουν ανακαλυφθεί καθ' όλη την διάρκεια της ύπαρξης του, θεωρείται ακόμα από τους ασφαλής αλγόριθμους.

RC2, RC4, RC5

Ο RC2 είναι ένας block cipher με κλειδί μεταβλητού μήκους που σχεδιάστηκε από τον Ron Rivest για την RSA Inc. Τα αρχικά σημαίνουν "Ron's Code" ή "Rivest's Cipher". Είναι γρηγορότερος από τον DES και στόχος της σχεδίασης ήταν να λειτουργήσει για αντικατάσταση του DES. Μπορεί να γίνει περισσότερο ή λιγότερο ασφαλής από τον DES, ανάλογα με το μήκος του κλειδιού. Έχει μέγεθος block ίσο με 64 bits και είναι έως και τρεις φορές ταχύτερος από τον DES.

Ο RC4 είναι ένας stream cipher που σχεδιάστηκε πάλι από την Ron Rivest για λογαριασμό της RSA Inc. Έχει μεταβλητό μήκος κλειδιού και λειτουργεί στο επίπεδο του byte. Θεωρείται εξαιρετικά ασφαλής και οι υλοποιήσεις του σε λογισμικό τρέχουν πολύ γρήγορα. Χρησιμοποιείται για κρυπτογράφηση τοπικά αποθηκευμένων αρχείων και για την διασφάλιση της επικοινωνίας μεταξύ δύο απομακρυσμένων σημείων μέσω του πρωτοκόλλου SSL.

Ο RC5 είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο αριθμός των επαναλήψεων μπορεί να είναι από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.

Ο αλγόριθμος IDEA (International Data Encryption Algorithm)

Ο IDEA σχεδιάστηκε από δύο ερευνητές στην Ελβετία, οπότε δεν έχει την καθοδήγηση της NSA. Χρησιμοποιεί ένα κλειδί 128 bit οπότε δεν μπορεί να παραβιαστεί χρησιμοποιώντας μεγάλη υπολογιστική ισχύ, για τα σημερινά δεδομένα

αλλά και για τις επόμενες δεκαετίες. Σήμερα δεν υπάρχει γνωστός αλγόριθμος ή συσκευή που να μπορεί να παραβιάσει το IDEA.
Η βασική δομή του αλγορίθμου μοιάζει με το DES στο γεγονός ότι στην είσοδο δέχεται 64 bit καθαρού κειμένου που παραμετροποιούνται με συνεχείς επαναλήψεις και στην έξοδο παράγει 64 bit κρυπτογραφημένου κειμένου. Επειδή η πολυπλοκότητα κάθε επανάληψης είναι μεγαλύτερη από το DES, ο IDEA χρειάζεται μόνο οκτώ επαναλήψεις. Ο αλγόριθμος μιας επανάληψης είναι ένας συνδυασμός πράξεων πάνω στις τέσσερις 16-αδες bit που αποτελούν μια είσοδο των 64 bit.

ΓΕΝΙΚΑ

5.4.2 ΑΣΥΜΜΕΤΡΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

Εισαγωγή για την Ασύμμετρη Κρυπτογραφία

Διαφορετικά κλειδιά χρησιμοποιούνται στην ασύμμετρη κρυπτογραφία, για την κρυπτογράφηση και την αποκρυπτογράφηση, το δημόσιο (public) και το ιδιωτικό (private) κλειδί αντίστοιχα (Σχήμα 5.4). Τα κλειδιά αυτά παράγονται έτσι ώστε να έχουν τις εξής ιδιότητες:

- Μήνυμα κρυπτογραφημένο με το δημόσιο κλειδί μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί και αντίστροφα.
- Το ένα κλειδί δεν μπορεί να προκύψει από το άλλο με απλό τρόπο.

Το 1976 οι Diffie και Hellman διατύπωσαν την βασική αρχή της κρυπτογραφίας δημόσιου κλειδιού, ενώ το 1977 οι Rivest, Shamir και Adleman δημιούργησαν το κρυπτοσύστημα RSA, την πρώτη υλοποίηση συστήματος κρυπτογραφίας δημοσίου κλειδιού, βασιζόμενοι σε αρχές της θεωρίας των πεπερασμένων πεδίων.

Για να αποκατασταθεί η επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας, ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά, ένα δημόσιο και ένα ιδιωτικό. Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και

να κρυπτογραφήσει το μήνυμα με αυτό. Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί.

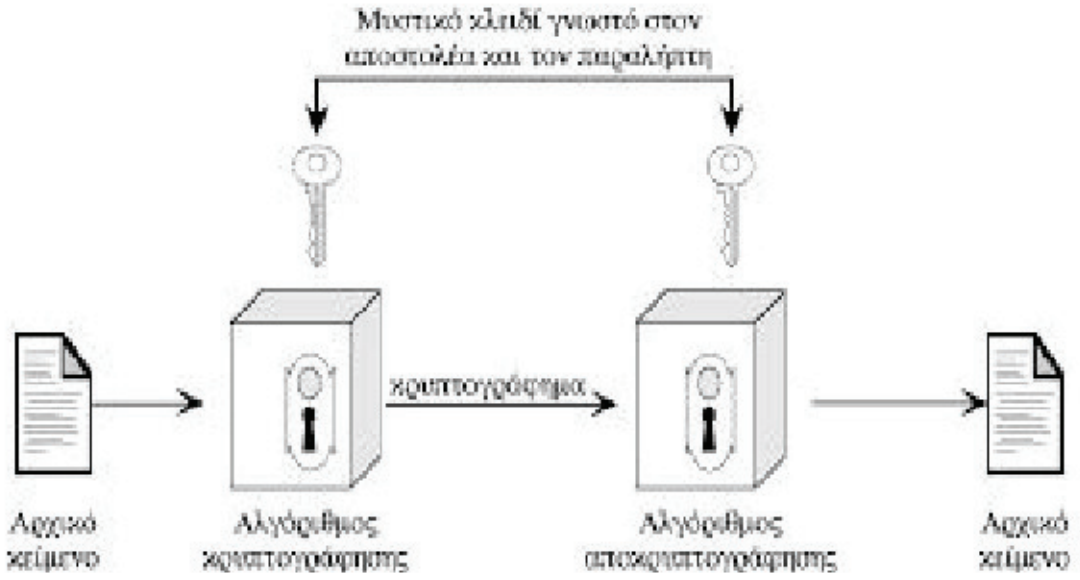
Το δημόσιο κλειδί δεν αποτελεί μυστική πληροφορία κι έτσι μπορεί να μεταδοθεί χωρίς την απαίτηση ύπαρξης ασφαλούς μέσου. Το ιδιωτικό κλειδί χρησιμοποιείται μόνο από τον ιδιοκτήτη του και δε μεταδίδεται ποτέ. Όταν ένα μήνυμα έχει κρυπτογραφηθεί με το δημόσιο κλειδί κάποιου χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο με το ιδιωτικό του κλειδί. Και επειδή μόνο ο ίδιος ο χρήστης γνωρίζει το ιδιωτικό του κλειδί, μόνο αυτός μπορεί να αποκρυπτογραφήσει τα μηνύματα που απευθύνονται σε αυτόν. Ούτε καν το δημόσιο κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα, κι έτσι η γνώση του δημόσιου κλειδιού από τρίτους δεν αποτελεί πρόβλημα.

Η ασύμμετρη κρυπτογραφία προσφέρει μεγαλύτερη ασφάλεια από τη συμμετρική. Έχει όμως το μειονέκτημα ότι οι αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι πολύ πιο αργοί από τους αλγόριθμους συμμετρικής κρυπτογράφησης.

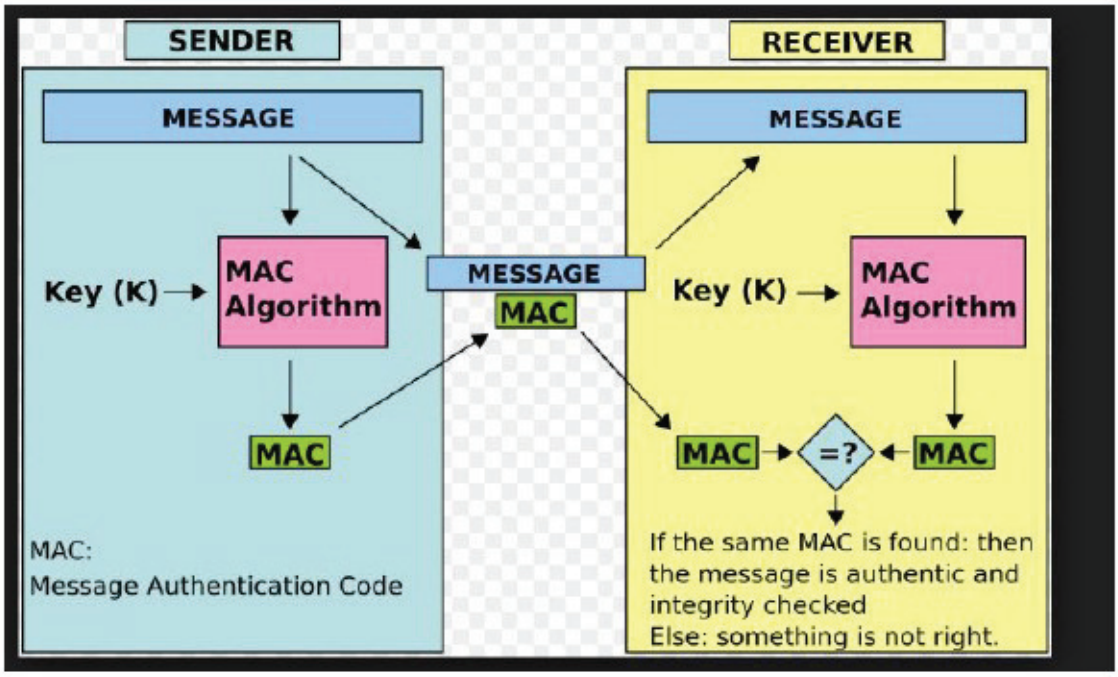
Ασύμμετρα Κρυπτοσυστήματα και Αυθεντικοποίηση Μηνυμάτων

Η κρυπτογράφηση έχει σαν σκοπό την προστασία από παθητικές επιθέσεις (passive attacks) και ενεργητικές επιθέσεις (active attacks). Οι παθητικές επιθέσεις στοχεύουν στην παραβίαση της εμπιστευτικότητας μηνυμάτων (eavesdropping) και οι ενεργητικές επιθέσεις κατά των μεταδιδόμενων δεδομένων και δοσοληψιών (falsification of data and transactions). Η υπηρεσία ασφάλειας η οποία παρέχει προστασία από τέτοιες κατηγορίες επιθέσεων, είναι γνωστή ως αυθεντικοποίηση μηνυμάτων (message authentication).
Η αυθεντικοποίηση μηνυμάτων είναι μία διαδικασία που επιτρέπει στους χρήστες μια ασφαλή ακεραιότητα (integrity), δηλαδή τη μη τροποποίηση των δεδομένων του μηνύματος, επισημαίνοντας την αυθεντικότητα (authenticity) της πηγής μετάδοσης. Αν το μήνυμα περικλείει και χρονοσήμανση (timestamp) διασφαλίζεται το γεγονός ότι το μήνυμα δεν έχει καθυστερήσει πέραν ενός "φυσιολογικού" ορίου και ότι δεν αποτελεί αναμετάδοση παλαιότερου μηνύματος. Υπάρχουν δυο περιπτώσεις στην αυθεντικοποίηση μηνυμάτων το πώς θα γίνει η μετάδοση του μηνύματος

⇥ Η Συμβατική Κρυπτογράφηση χρησιμοποιώντας την αυθεντικοποίηση είναι δυνατόν να επιτευχθεί απλώς με την χρήση της. Π.χ. έχουμε ένα μυστικό κλειδί το οποίο διαμοιράζονται ο αποστολέας και ο παραλήπτης τότε μόνο ο αυθεντικός αποστολέας θα είναι σε θέση να κρυπτογραφήσει το μήνυμα επιτυχώς.

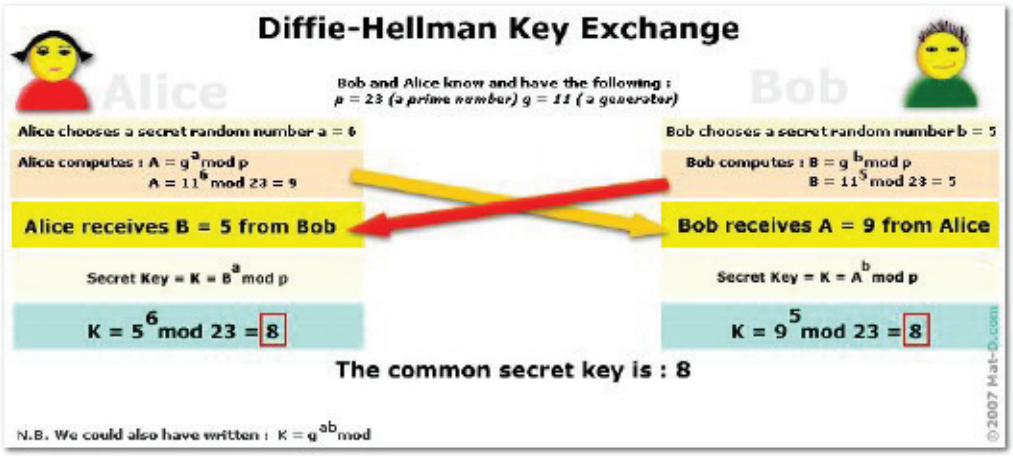


Αυθεντικοποίηση μηνυμάτων χωρίς κρυπτογράφηση παράγει μία ετικέτα μηνύματος (authentication tag), η οποία ενσωματώνει το μήνυμα προς μετάδοση το οποίο δεν είναι κρυπτογραφημένο μπορεί να είναι αναγνώσιμο στον προορισμό ανεξάρτητα από τη μέθοδο αυθεντικοποίησης στον προορισμό του.



Αλγόριθμοι για την Διαχείριση και Ανταλλαγή Κλειδιών

Diffie-Hellman



Το πρωτόκολλο Diffie-Hellman είναι ένας μηχανισμός ανταλλαγής κλειδιών και αναπτύχθηκε από τους Diffie και Hellman το 1976. Επιτρέπει σε δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές δίκτυο.

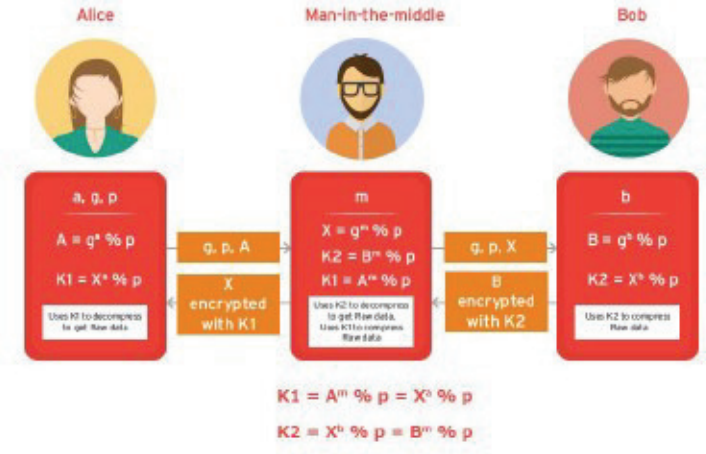
Το πρωτόκολλο έχει δύο παραμέτρους: p και g.

Είναι και οι δύο δημοσιοποιημένοι και μπορούν να χρησιμοποιηθούν από όλους τους χρήστες του συστήματος.

Η παράμετρος p είναι ένας πρώτος αριθμός και η παράμετρος g είναι ένας ακέραιος με την εξής ιδιότητα: για οποιοδήποτε ακέραιο αριθμό n στο διάστημα [1, p-1],

υπάρχει αριθμός k τέτοιος ώστε $g^{k} = n \bmod p$.

Οι πρώτες εκδόσεις του μηχανισμού Diffie-Hellman ήταν ευάλωτες σε επιθέσεις man-in-the-middle. Σε αυτή την επίθεση ο χρήστης C παρεμβάλλεται στην επικοινωνία των A και B και όταν ανταλλάσσουν τις δημόσιες τιμές τους τις αντικαθιστά με τις δικές του. Δηλαδή όταν ο A μεταδίδει την δημόσια τιμή του στον B, ο C την αντικαθιστά με την δικιά του και την στέλνει στον B. Ομοίως όταν ο B στέλνει την δημόσια τιμή του στον A. Σαν συνέπεια, οι C και A συμφωνούν για ένα μυστικό κλειδί και οι C και B συμφωνούν για ένα άλλο κλειδί. Έτσι ο C μπορεί να διαβάσει τα μηνύματα που μεταδίδουν ο A στον B και πιθανώς να τα τροποποιήσει πριν τα προωθήσει σε έναν από τους δύο.



Το 1992 αναπτύχθηκε μία ανανεωμένη έκδοση από τους Diffie, Van Oorschot και Wiener που υποστήριζε την πιστοποίηση της ταυτότητας των δύο πλευρών και είχε σαν σκοπό να καταπολεμήσει την επίθεση man-in-the-middle. Τα μηνύματα ανταλλάσσονται υπογεγραμμένα με τις ιδιωτικές κλείδες των A και B, ενώ χρησιμοποιούνται και πιστοποιητικά για την απόκτηση των σωστών δημοσίων κλείδων. Ο C ακόμα και αν είναι σε θέση να παρακολουθεί την επικοινωνία των A και B, δεν μπορεί να πλαστογραφήσει τα μηνύματα.

Αλγόριθμοι για Ασύμμετρα Κρυπτοσυστήματα

Οι πιο διαδεδομένοι αλγόριθμοι για ασύμμετρα κρυπτοσυστήματα είναι ο αλγόριθμος RSA και ο αλγόριθμος των Diffie-Hellman. Υπάρχουν επίσης και άλλοι δυο αλγόριθμοι ο Digital Signature Standard (DSS) και ο Elliptic- Curve Cryptography(ECC).

Αλγόριθμος RSA

Το 1977 αναπτύχθηκε ένα από τα πρώτα ασύμμετρα κρυπτοσυστήματα από τους R. Rivest, A. Shamir και L. Adleman στο MIT και το οποίο δημοσιεύτηκε για πρώτη φορά το 1978. Το RSA κυριάρχησε ως η πλέον μοναδική ευρέως αποδεκτή και εύκολα υλοποιημένη προσέγγιση για της κρυπτογράφησης των ασύμμετρων κρυπτοσυστημάτων. Ο RSA είναι αλγόριθμος κρυπτογράφησης στον οποίο το αρχικό και το κρυπτογραφημένο κείμενο είναι ακέραιοι αριθμοί με τιμές μεταξύ 0 και n-1, για κάποιο n.
Η κρυπτογράφηση και η αποκρυπτογράφηση είναι της ακόλουθης μορφής για ένα αρχικό κείμενο M και για το αντίστοιχο κρυπτογραφημένο C συμβολίζονται ως ακολούθως:

$$C = M^{e} \bmod n$$

$$M = C^{d} \bmod n = (M^{e})^{d} \bmod n = M^{ed} \bmod n$$

Τόσο ο αποστολέας όσο και ο παραλήπτης θα πρέπει να γνωρίζουν τις τιμές των n και e και μόνον ο παραλήπτης πρέπει να γνωρίζει την τιμή του d. Ουσιαστικά ο RSA είναι ένας αλγόριθμος" για ασύμμετρο κρυπτοσύστημα με δημόσιο κλειδί KU={e,n} και ιδιωτικό κλειδί KR={d,n}. Για να είναι ικανοποιητικός αυτός ο αλγόριθμος για κρυπτογράφηση δημοσίου κλειδιού θα πρέπει να ικανοποιούνται οι ακόλουθες απαιτήσεις:

- Είναι δυνατό να βρεθούν τιμές για τα e,d,n τέτοιες ώστε να ισχύει: $M = M^{ed} \bmod n$, για κάθε M<n.
- Είναι σχετικά εύκολο να υπολογιστούν τα M και C^{e} , για C^{d} κάθε M<n.
- Είναι αδύνατο να προσδιοριστεί το d, δοθέντων των e και n.

Οι δύο πρώτες απαιτήσεις ικανοποιούνται εύκολα. Η τρίτη απαίτηση μπορεί να ικανοποιηθεί μόνο για μεγάλες τιμές των e και n.

5.5 ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΗς ΣΥΜΜΕΤΡΙΚΗΣ ΚΑΙ ΑΣΥΜΜΕΤΡΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς να διαρρεύσει σε τρίτους, είναι το μεγαλύτερο πρόβλημα της συμμετρικής κρυπτογραφίας. Η μετάδοση μέσα από το Διαδίκτυο δεν είναι ασφαλής καθώς οποιοσδήποτε γνωρίζει για την συναλλαγή και διαθέτει τα κατάλληλα μέσα, μπορεί να την καταγράψει και να αποκτήσει το κλειδί. Κατέχοντας το κλειδί, μπορεί να διαβάσει, να τροποποιήσει και να πλαστογραφήσει όλα τα μηνύματα που ανταλλάσσουν οι δύο ανυποψίαστοι χρήστες. Η επικοινωνία

για την μετάδοση του κλειδιού μπορεί να πραγματοποιηθεί με τη χρήση και άλλων μέσων (π.χ. τηλεφωνία), αλλά και πάλι δεν μπορεί να διασφαλιστεί η απόρρητη επικοινωνία των χρηστών. Η ασύμμετρη κρυπτογραφία δίνει λύση σε αυτό το πρόβλημα αφού σε καμία περίπτωση δεν "ταξιδεύουν" σ το δίκτυο οι εν λόγω ευαίσθητες πληροφορίες.
Η παροχή ψηφιακών υπογραφών που δεν μπορούν να αποκηρυχθούν από την πηγή τους είναι ακόμη ένα από τα πλεονεκτήματα των ασύμμετρων κρυπτοσυστημάτων. Η πιστοποίηση ταυτότητας μέσω της συμμετρικής κρυπτογράφησης απαιτεί την κοινή χρήση του ίδιου κλειδιού και πολλές φορές τα κλειδιά αποθηκεύονται σε υπολογιστές που κινδυνεύουν από εξωτερικές επιθέσεις. Το αποτέλεσμα είναι ότι ο αποστολέας μπορεί να αποκηρύξει ένα πρωτύτερα υπογεγραμμένο μήνυμα, υποστηρίζοντας ότι το μυστικό κλειδί είχε κατά κάποιον τρόπο αποκαλυφθεί. Στην ασύμμετρη κρυπτογραφία δεν υφίσταται τέτοιος κίνδυνος, καθώς μόνο ο ίδιος ο χρήστης γνωρίζει την ιδιωτική του κλείδα και είναι αποκλειστική ευθύνη του η φύλαξη της.
Μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ταχύτητα. Κατά κανόνα, η διαδικασίες κρυπτογράφησης και πιστοποίησης ταυτότητας με συμμετρικό κλειδί είναι σημαντικά ταχύτερη από την κρυπτογράφηση και ψηφιακή υπογραφή με ζεύγος ασύμμετρων κλειδιών. Η ιδιότητα αυτή καλείται διασφάλιση της μη αποκήρυξης της πηγής (non-repudiation). Επίσης, τεράστιο μειονέκτημα της ασύμμετρης κρυπτογραφίας είναι η ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλείδων από οργανισμούς (Certificate Authority) ώστε να διασφαλίζεται η κατοχή τους νόμιμους χρήστες. Όταν κάποιος απατεώνας κατορθώσει και ξεγελάσει τον οργανισμό, μπορεί να συνδέσει το όνομα του με την δημόσια κλείδα ενός νόμιμου χρήστη και να προσποιείται την ταυτότητα αυτού του νόμιμου χρήστη. Σε μερικές περιπτώσεις, η ασύμμετρη κρυπτογραφία δεν είναι απαραίτητη και η συμμετρική κρυπτογραφία από μόνη της είναι αρκετή. Τέτοιες περιπτώσεις είναι περιβάλλονται κλειστά, που δεν έχουν σύνδεση με το Διαδίκτυο.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΚΑΙ ΜΕΙΟΝΕΚΤΗΜΑΤΑ ΤΩΝ ΜΕΘΟΔΩΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ

Συμμετρική κρυπτογράφηση	Ασύμμετρη κρυπτογράφηση
(-) Η συνεννόηση και ανταλλαγή του κλειδιού, χωρίς κάποιος τρίτος να μάθει για αυτό.	(+) Παρέχουν ψηφιακές υπογραφές που δεν μπορούν να αποκηρυχθούν από την πηγή τους.
(+) Η κρυπτογράφηση πραγματοποιείται με ταχύτατους ρυθμούς.	(-) Έλλειψη ταχύτητας.
(+) Δεν υπάρχει ανάγκη για πιστοποίηση των κλειδιών.	(-) Ανάγκη για πιστοποίηση και επαλήθευση των δημόσιων κλειδών από οργανισμούς.

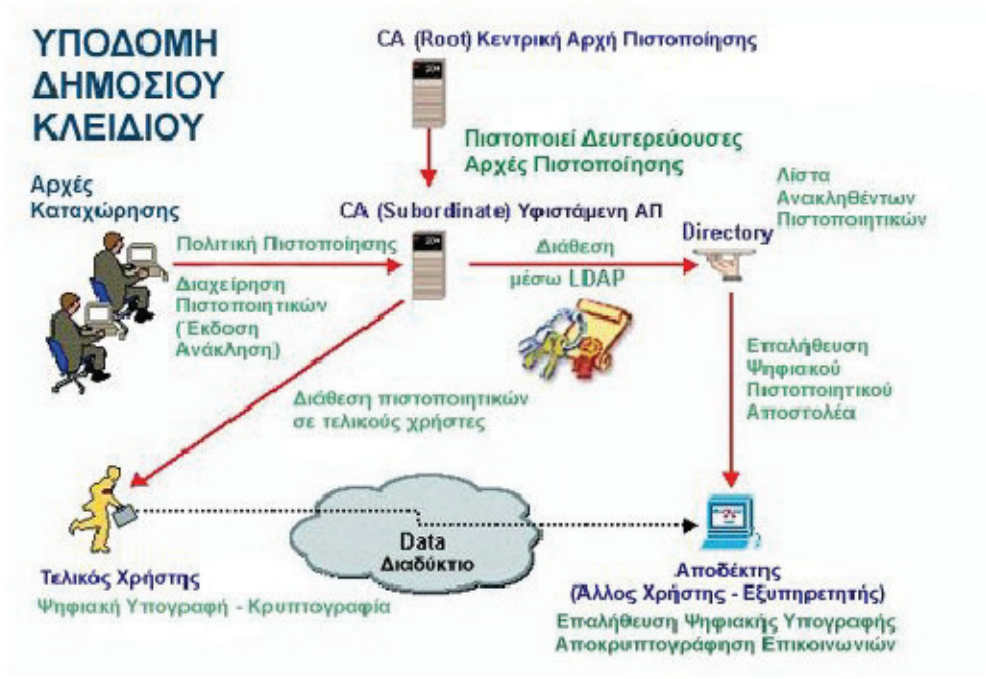
ΚΕΦΑΛΑΙΟ 6

ΠΙΣΤΟΠΟΙΗΣΗ ΑΥΘΕΝΤΙΚΟΤΗΤΑΣ

6.1 Η ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Εισαγωγή

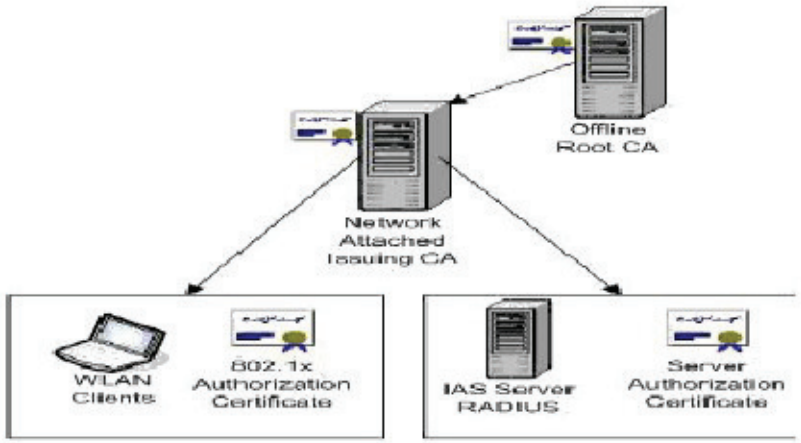
Η αλματώδης ανάπτυξη του Διαδικτύου τις τελευταίες δεκαετίες άνοιξε νέους ορίζοντες στον τομέα της επικοινωνίας αλλά και της διακίνησης των πληροφοριών. Εκατομμύρια χρήστες σε όλο τον κόσμο απολαμβάνουν τις διευκολύνσεις που τους παρέχει ο Παγκόσμιος Ιστός: ανταλλάσσουν δεδομένα και πληροφορίες, επικοινωνούν μεταξύ τους με χρήση του ηλεκτρονικού ταχυδρομείου, διεκπεραιώνουν τραπεζικές συναλλαγές, κάνουν αγορές, αποπληρώνουν ακόμα και τους φόρους τους. Επίσης, οι επιχειρήσεις βρήκαν στο Διαδίκτυο ένα ισχυρό εργαλείο προβολής. Κάθε επιχείρηση που θέλει να παραμείνει ανταγωνιστική, χρησιμοποιεί την ιστοσελίδα της για την παρουσίαση των επιχειρηματικών της δραστηριοτήτων, την εδραίωση νέων δεσμών με τους πελάτες σε μια παγκόσμια αγορά, την αύξηση της παραγωγικότητας της και τη μείωση του λειτουργικού της κόστους.Καταλαβαίνει λοιπόν κανείς, ότι στο ανταγωνιστικό και μη ασφαλές περιβάλλον του Διαδικτύου, η ανάγκη προστασίας των διακινούμενων πληροφοριών προβάλλει επιτακτική. Η λύση βρίσκεται στην ανάπτυξη μιας Υποδομής Δημοσίου Κλειδιού (Public Key Infrastructure, PKI). Η Υποδομή Δημοσίου Κλειδιού είναι μία υποσχόμενη νέα τεχνολογία για τη παροχή ασφάλειας στις πληροφορίες που διακινούνται, όχι μόνο μέσω του Διαδικτύου, αλλά και μέσω των ιδιωτικών δικτύων επιχειρήσεων και οργανισμών.
Ως Υποδομή Δημοσίου Κλειδιού (PKI) ορίζεται ο συνδυασμός του υλικού, λογισμικού, μηχανισμών κρυπτογράφησης, πολιτικών ασφαλείας και υπηρεσιών που απαιτούνται για τη δημιουργία, αποθήκευση, διανομή και διαχείριση κλειδιών και ψηφιακών πιστοποιητικών. Μία σωστά υλοποιημένη Υποδομή Δημοσίου Κλειδιού παρέχει όλους τους απαραίτητους μηχανισμούς μέσω των οποίων ικανοποιούνται οι θεμελιώδεις απαιτήσεις για εμπιστευτικότητα, πιστοποίηση αυθεντικότητας, έλεγχο ακεραιότητας και μη αποκήρυξη.
Έτσι η ΥΔΚ παρέχει το απαραίτητο πλαίσιο για την ανάπτυξη μιας σειράς εφαρμογών (PKI enabled applications) όπως είναι η ασφαλής ανταλλαγή μηνυμάτων μέσω ηλεκτρονικού ταχυδρομείου, η δημιουργία Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networks, VPN), το Single Sign On (SSO) σε εταιρικές εφαρμογές και η πιστοποίηση αυθεντικότητας για απομακρυσμένη πρόσβαση (remote access).



6.2 ΣΥΣΤΑΤΙΚΑ ΜΕΡΗ ΥΠΟΔΟΜΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

6.2.1 Αρχή Πιστοποίησης (Certification authority-CA)

Κύρια λειτουργία της Αρχής Πιστοποίησης (CA), ή αλλιώς Αρχής Έκδοσης, είναι να πιστοποιεί την αυθεντικότητα των οντοτήτων που λαμβάνουν μέρος σε μία ηλεκτρονική συναλλαγή. Για να το πετύχει αυτό η Αρχή Πιστοποίησης εκδίδει ένα ψηφιακό πιστοποιητικό. Στα πλαίσια του PKI, πιστοποίηση είναι η διαδικασία της συσχέτισης της ταυτότητας ενός χρήστη και ενδεχομένως άλλων πληροφοριών με ένα δημόσιο κλειδί. Το αποτέλεσμα της πιστοποίησης είναι ένα πιστοποιητικό δημοσίου κλειδιού το οποίο υπογράφεται ψηφιακά από το ιδιωτικό κλειδί της Αρχής Πιστοποίησης. Η ψηφιακή υπογραφή των πιστοποιητικών με το ιδιωτικό κλειδί της Αρχής Πιστοποίησης εξασφαλίζει την ακεραιότητα τους.



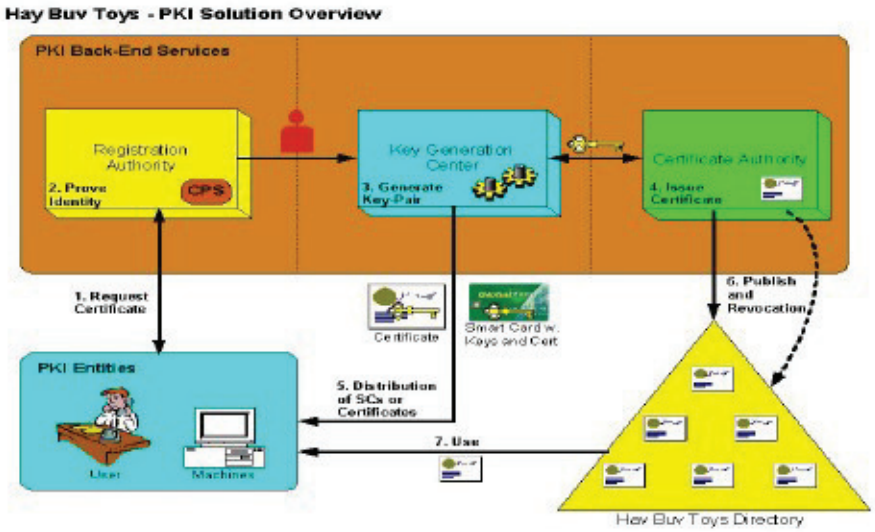
6.2.2 Αρχή Καταχώρησης (Registration Authority-RA)

Επειδή τις περισσότερες φορές υπάρχει πληθώρα αιτήσεων πιστοποιητικών, είναι δύσκολο για την Αρχή Πιστοποίησης να δέχεται τα αιτήματα, να εξακριβώνει την εγκυρότητά τους και τέλος να εκδίδει τα πιστοποιητικά. Η Αρχή Καταχώρησης (RA) είναι ο μεσολαβητής ανάμεσα στον πελάτη που αιτείται ένα ψηφιακό πιστοποιητικό και την Αρχή Πιστοποίησης. Απαραίτητη προϋπόθεση είναι φυσικά ότι η Αρχή Πιστοποίησης εμπιστεύεται την Αρχή Καταχώρησης. Οι λειτουργίες που εκτελούνται από την Αρχή Καταχώρησης είναι οι παρακάτω:

- Λαμβάνει τις αιτήσεις των πελατών και επαληθεύει την εγκυρότητα των στοιχείων τους. Τα στοιχεία αυτά είναι συνήθως το όνομα και το επώνυμο του πελάτη, η ηλεκτρονική του διεύθυνση και το όνομα της εταιρίας ή του οργανισμού στο οποίο εργάζεται. Η επαλήθευση των στοιχείων είναι συνήθως μια διαδικασία που λαμβάνει χώρα πρόσωπο με πρόσωπο και στην οποία χρησιμοποιούνται επίσημα έγγραφα που επαληθεύουν ότι ο πελάτης είναι πράγματι αυτός που ισχυρίζεται ότι είναι (π.χ μια ταυτότητα).
- Στέλνει της αιτήσεις στην Αρχή Πιστοποίησης.
- Λαμβάνει τα πιστοποιητικά από την Αρχή Πιστοποίησης.
- Στέλνει τα πιστοποιητικά στους αντίστοιχους πελάτες.

Οι λειτουργίες της Αρχής Καταχώρησης θα μπορούσαν να είναι μέρος της Αρχής Πιστοποίησης. Όμως, επειδή οι λειτουργίες αυτές απαιτούν εντατική επεξεργασία δεδομένων, η διεκπεραίωση τους από μια μοναδική αρχή θα μπορούσε να είναι εξαιρετικά χρονοβόρα και οικονομικά ασύμφορη. Ο πρωταρχικός στόχος της Αρχής Καταχώρησης είναι να αποφορτίσει την Αρχή Πιστοποίησης από το βάρος δύσκολων λειτουργιών έτσι ώστε να είναι εφικτή η κλιμάκωση της μεθόδου έκδοσης πιστοποιητικών και φυσικά η μείωση του λειτουργικού της κόστους. Η Αρχής Καταχώρησης, κυρίως για λόγους ασφαλείας, δεν μπορεί ποτέ και με κανέναν τρόπο να εκδώσει πιστοποιητικά και λίστες πιστοποιητικών (CRLs).

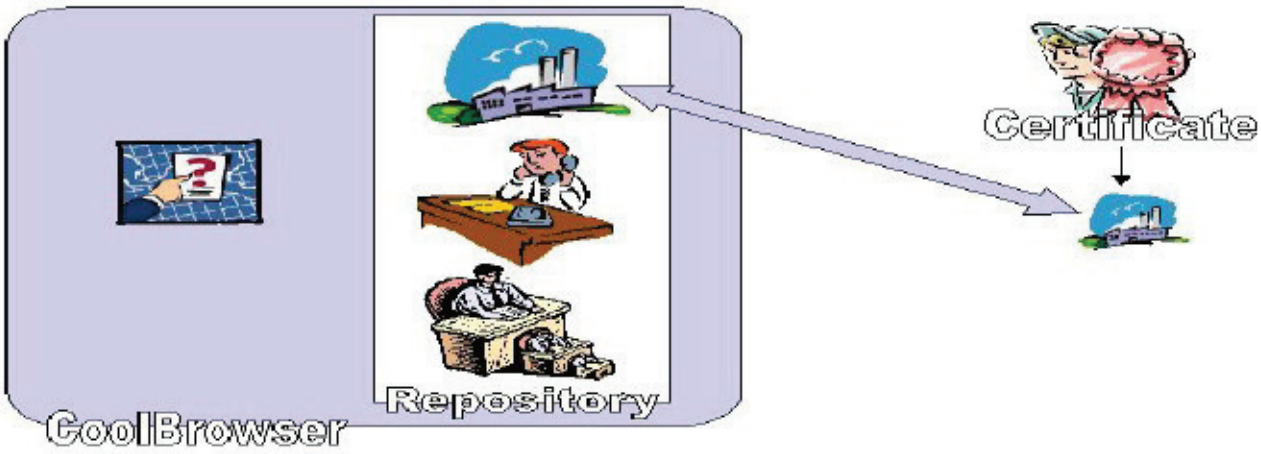
Στις περιπτώσεις μεγάλων υποδομών PKI όπου το πλήθος των χρηστών είναι πολύ μεγάλο και λογικά διασκορπισμένο σε μια ευρύτερη γεωγραφική περιοχή, τη διαδικασία της επαλήθευσης των δεδομένων αναλαμβάνουν οι επιμέρους Τοπικές Αρχές Καταχώρησης (Local Registration Authority-LRA). Έτσι οι χρήστες διευκολύνονται από τη δυνατότητα πρόσβασης σε μια LRA κοντά στον τόπο διαμονής τους, η οποία φροντίζει για τη σωστή λειτουργία της υποδομής.



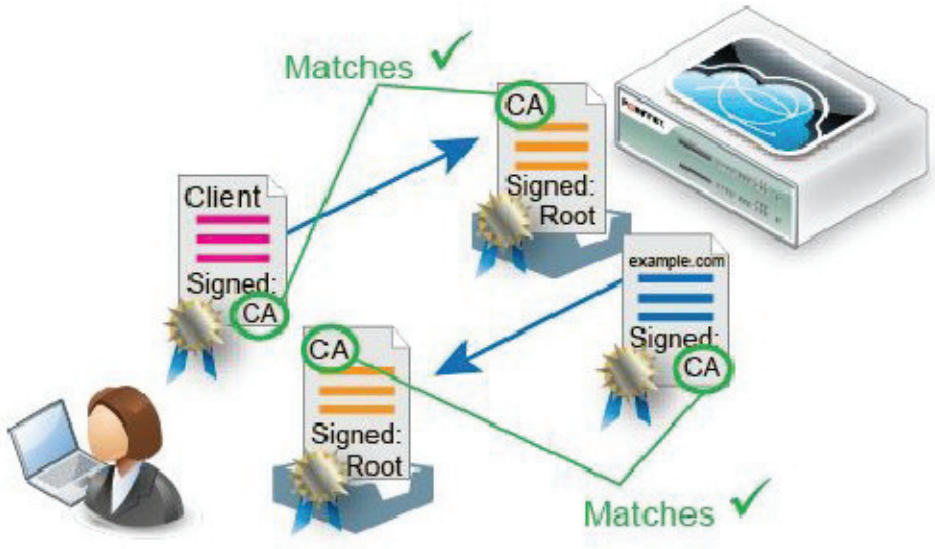
6.2.3 Αποθήκη Πιστοποιητικών (Certificate Repository)

Από τη στιγμή που θα εκδοθεί ένα πιστοποιητικό θα πρέπει να μπορεί να διανεμηθεί στους χρήστες και στους οργανισμούς που ανήκουν στο δίκτυο. Η αποθήκη πιστοποιητικών είναι ο χώρος στον οποίο η Αρχή Έκδοσης αποθηκεύει τα πιστοποιητικά και τις λίστες πιστοποιητικών (CRLs) που εκδίδει. Πιο συχνά αναφερόμαστε στον όρο αποθήκη πιστοποιητικών με τον όρο κρυπτογραφικός εξυπηρετητής (cryptographic server). Τα πιστοποιητικά μπορούν να διανεμηθούν με δύο τρόπους ανάλογα με το είδος της υποδομής PKI που εφαρμόζεται. Συγκεκριμένα τα πιστοποιητικά μπορούν να διανέμονται είτε από τους ίδιους τους χρήστες είτε από έναν εξυπηρετητή καταλόγου που χρησιμοποιεί τη μορφή καταλόγου LDAP (Lightweight Directory Access Protocol) για την εύρεση πληροφοριών που αποθηκεύονται σε μια X.500 βάση δεδομένων. Η αποθήκη των πιστοποιητικών θα πρέπει να είναι σε θέση να:

- Πιστοποιεί την ισχύ των δημοσίων κλειδιών υπογράφοντας ψηφιακά το δημόσιο κλειδί.
- Αποσύρει χαμένα ή χρονικά ληγμένα κλειδιά.
- Δημοσιεύει τα δημόσια κλειδιά στον εξυπηρετητή δημοσίου καταλόγου.



6.2.4 Πελάτες Υποδομής Δημόσιου Κλειδιού (PKI Clients)



Οι οντότητες οι οποίες κάνουν αίτηση σεμια Αρχή Πιστοποίησης ή Αρχή Καταχώρησης RA για την έκδοση πιστοποιητικών ονομάζονται πελάτες Υποδομής Δημοσίου Κλειδιού (PKI clients). Για να αποκτήσει ένα ψηφιακό πιστοποιητικό από μια Αρχή Πιστοποίησης ο πελάτης PKI θα πρέπει να ακολουθήσει τα παρακάτω βήματα:

- Αποστολή μιας αίτησης για τη δημιουργία ενός ζεύγους δημόσιου-ιδιωτικού κλειδιού. Το ζεύγος των κλειδιών μπορεί να δημιουργεί είτε από την Αρχή Πιστοποίησης από τον ίδιο το χρήστη. Τα κλειδιά που θα δημιουργηθούν περιέχουν πληροφορίες για τον χρήστη.
- Αφού έχει δημιουργηθεί το ζεύγος των κλειδιών, ο χρήστης θα πρέπει να στείλει στην Αρχή Πιστοποίησης μια αίτηση για έκδοση ψηφιακού πιστοποιητικού. Αυτό μπορεί να γίνει μέσω μιας Αρχής Καταχώρησης.
- Αφού ο πελάτης λάβει το πιστοποιητικό από την Αρχή Πιστοποίησης είναι σε θέση να πιστοποιήσει την αυθεντικότητά του μέσα σε ένα επικοινωνιακό σύστημα.

Όλη η επικοινωνία μεταξύ του πελάτη και της Αρχής Πιστοποίησης κρατείται μυστική. Επίσης, ο πελάτης είναι υπεύθυνος για την ασφάλεια του ιδιωτικού του κλειδιού. Σε περίπτωση που το ιδιωτικό κλειδί χαθεί τότε τα κρυπτογραφημένα μηνύματα δεν θα μπορούν να αποκρυπτογραφηθούν. Ακόμη, σε περίπτωση που το ιδιωτικό κλειδί υποπέσει στην ιδιοκτησία κάποιας μη εξουσιοδοτημένης οντότητας, τότε εκείνη θα είναι σε θέση να αποκρυπτογραφήσει οποιοδήποτε μήνυμα. Γίνεται λοιπόν προφανές ότι η ασφάλεια του ιδιωτικού κλειδιού είναι πολύ σημαντική. Ένας χρήστης μπορεί να διασφαλίσει τη μυστικότητα του ιδιωτικού του κλειδιού χρησιμοποιώντας διάφορες συσκευές υλικού όπως είναι τα tokens και οι έξυπνες

κάρτες. Ένα token είναι μια φορητή συσκευή που χρησιμοποιείται για να πιστοποιήσει την αυθεντικότητα ενός χρήστη που εισέρχεται σε ένα δίκτυο. Μια έξυπνη κάρτα μοιάζει πολύ με μία πιστωτική κάρτα, με τη διαφορά ότι έχει ενσωματωμένο έναν μικροεπεξεργαστή κατάλληλο για αποθήκευση πληροφοριών. Πρόσβαση στη λειτουργία της κάρτας έχει μόνο εκείνος ο χρήστης που κατέχει το κατάλληλο κωδικό PIN (Personal Identification Number).

6.3 ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ (Digital Certificates)

6.3.1 Εισαγωγή

Η βασική αρχή που επιτρέπει στην τεχνολογία δημοσίου κλειδιού να κλιμακώνεται είναι το γεγονός, ότι τα δημόσια κλειδιά μπορούν να είναι ελεύθερα διαθέσιμα ανάμεσα σε ένα σύνολο οντοτήτων που θέλει να τα χρησιμοποιήσει για να κάνει χρήση υπηρεσιών ασφαλείας, όπως είναι η κρυπτογράφηση και η αποκρυπτογράφηση δεδομένων και η ψηφιακή υπογραφή.
Γίνεται εύκολα αντιληπτό ότι για να μπορέσει να λειτουργήσει σωστά μια τέτοια τεχνολογία θα πρέπει να πληρούνται δύο βασικές προϋποθέσεις:
- Η διασφάλιση της ακεραιότητας του δημοσίου κλειδιού
- Η αξιόπιστη σύνδεση του δημοσίου κλειδιού με το νόμιμο κάτοχο του.

Σε ένα περιβάλλον Υποδομής Δημοσίου Κλειδιού οι δύο παραπάνω προϋποθέσεις πληρούνται με τη χρήση των ψηφιακών πιστοποιητικών. Τα ψηφιακά πιστοποιητικά εκδίδονται από μία Τρίτη Έμπιστη Οντότητα (Trusted Third Party) που ονομάζεται Αρχή Έκδοσης Πιστοποιητικών (Certification authority-CA).
Ένα ψηφιακό πιστοποιητικό (digital certificate) , ή αλλιώς ένα πιστοποιητικό δημοσίου κλειδιού (public key certificate), είναι ένα ψηφιακά υπογεγραμμένο έγγραφο που συνδέει την τιμή ενός δημοσίου κλειδιού με την ταυτότητα μίας οντότητας (πρόσωπο, οργανισμός ή υπηρεσία) στην οποία ανήκει το συμπληρωματικό ιδιωτικό κλειδί. Υπογράφοντας το πιστοποιητικό, ηΑρχής Πιστοποίησης (CA) βεβαιώνει ότι το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί του πιστοποιητικού, βρίσκεται στην κατοχή της οντότητας που αναφέρεται στο πιστοποιητικό ,
Υπάρχουν διάφοροι τύποι ψηφιακών πιστοποιητικών μεταξύ των οποίων είναι:
- X.509 πιστοποιητικά δημοσίου κλειδιού
- SPKI (Simple Public Key Infrastructure) πιστοποιητικά
- PGP (Pretty Good Privacy) πιστοποιητικά

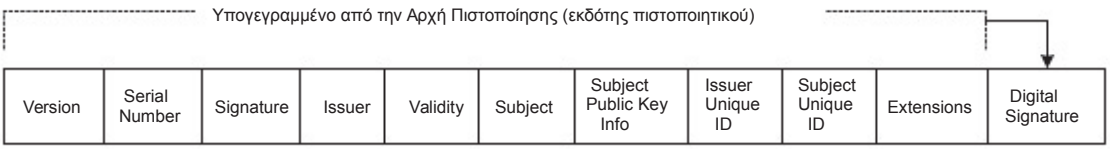
Καθένας από τους τύπους πιστοποιητικών που αναφέρονται παραπάνω έχουν διαφορετική δομή. Από τους παραπάνω τύπους πιστοποιητικών ο X.509 είναι εκείνος με την μεγαλύτερη αποδοχή και για αυτό στη συνέχεια θα εξεταστεί αναλυτικά η δομή του.

6.3.2 Πολιτική Πιστοποιητικού

Το πρότυπο X.509 ορίζει την Πολιτική Πιστοποιητικού (Certificate Policy) ως ένα σύνολο κανόνων που δηλώνουν την εφαρμογή ενός πιστοποιητικού σε μία συγκεκριμένη κοινότητα και/ή σε μία κλάση εφαρμογών με κοινές απαιτήσεις ασφάλειας. Για παράδειγμα, μία συγκεκριμένη πολιτική πιστοποιητικού μπορεί να δηλώνει την εφαρμογή ενός πιστοποιητικού για την πιστοποίηση αυθεντικότητας μιας ηλεκτρονικής μεταφοράς δεδομένων, τα οποία αφορούν το εμπόριο αγαθών μέσα σε ένα δοσμένο εύρος τιμής.
Αν και ο πρωταρχικός σκοπός μιας πολιτικής πιστοποιητικού είναι να ορίζει την πολιτική ασφαλείας που ακολουθείται από μία Αρχή Πιστοποίησης, μπορεί να χρησιμοποιηθεί και ως σημείο αναφοράς για άλλους οργανισμούς που θέλουν να αναπτύξουν μία σχέση εμπιστοσύνης με την συγκεκριμένη Αρχή Πιστοποίησης.
Δε θα πρέπει να γίνεται σύγχυση ανάμεσα στους όρους Πολιτική Πιστοποιητικού και Δήλωση Πρακτικών Πιστοποίησης (Certification Practice Statement - CPS) .
Η Δήλωση Πρακτικών είναι ένα κείμενο που περιγράφει πώς υλοποιούνται οι διαδικασίες και οι παρεχόμενες υπηρεσίες που περιγράφονται σε μια πολιτική πιστοποιητικού. Το κείμενο αυτό είναι πλήρες και εύκολο στην κατανόηση.

6.3.3 Δομή Πιστοποιητικού X.509

Το 1988 η Διεθνής Επιτροπή Τηλεπικοινωνιών (International Telecommunications Union-ITU) πρότεινε το πρότυπο X.509 για ψηφιακά πιστοποιητικά. Από τότε το X.509 έχει γίνει ένα de facto πρότυπο για την πιστοποίηση χρηστών σε ανοιχτά συστήματα όπως το Internet. Το πρότυπο X.509 για ψηφιακά πιστοποιητικά έχει παρουσιαστεί σε τρεις εκδόσεις με την τρίτη και τελευταία έκδοση, X.509v3, να είναι η περισσότερο εφαρμόσιμη. Η ευρεία αποδοχή της X.509v3 οφείλεται στη δυνατότητά της να συμπεριλαμβάνονται στο πιστοποιητικό πρόσθετα χαρακτηριστικά ανάλογα με την εφαρμογή που πρέπει να υλοποιηθεί.
Στο παρακάτω σχήμα παρουσιάζεται η γενική δομή ενός πιστοποιητικού X.509 τρίτης έκδοσης.



Σχήμα 6.1: Δομή ενός πιστοποιητικού X.509 τρίτης έκδοσης

Η λίστα που ακολουθεί επεξηγεί τα πεδία που παρουσιάζονται στο σχήμα 6.1 :
- Version: προσδιορίζει την έκδοση του πιστοποιητικού (v1,v2 ή v3)
- Serial Number: είναι ο σειριακός αριθμός ενός πιστοποιητικού. Ο αριθμός αυτός είναι μοναδικός για κάθε πιστοποιητικό που εκδίδεται από μια Αρχή Πιστοποίησης.
- Signature: προσδιορίζει τον αλγόριθμο με τον οποίο έχει δημιουργηθεί η

ψηφιακή υπογραφή του πιστοποιητικού.

- Issuer: προσδιορίζει το όνομα της Αρχής Πιστοποίησης που έχει υπογράψει και εκδώσει το πιστοποιητικό.
- Validity: περιλαμβάνει δύο ημερομηνίες ˙ την ημερομηνία από την οποία ξεκινάει η περίοδος ισχύος του πιστοποιητικού και την ημερομηνία στην οποία λήγει η περίοδος ισχύος του πιστοποιητικού.
- Subject: προσδιορίζει μοναδικά την οντότητα για την οποία εκδίδεται το πιστοποιητικό. Το πεδίο αυτό θα πρέπει να είναι πάντα μη μηδενικό.
- Subject Public Key Info: περιλαμβάνει το δημόσιο κλειδί καθώς και τον αλγόριθμο με τον οποίο μπορεί να χρησιμοποιηθεί το κλειδί.
- Issuer Unique ID: Το πεδίο αυτό είναι προαιρετικό και περιέχει ένα ID που χαρακτηρίζει μοναδικά τον εκδότη του πιστοποιητικού. Το πεδίο αυτό ισχύει μόνο για τις εκδόσεις 2 και 3.
- Subject Unique ID: το πεδίο αυτό είναι προαιρετικό και περιέχει ένα ID που προσδιορίζει μοναδικά τον ιδιοκτήτη του πιστοποιητικού. Το πεδίο αυτό ισχύει μόνο για τις εκδόσεις 2 και 3.
- Extensions: το πεδίο αυτό περιέχει τυχόν πρόσθετα χαρακτηριστικά του ψηφιακού πιστοποιητικού που ονομάζονται επεκτάσεις. Οι επεκτάσεις συναντώνται μόνο στην τρίτη έκδοση των X.509 πιστοποιητικών. Μια σημαντική ιδιότητα των επεκτάσεων είναι αυτή της κρισιμότητας. Πρόκειται για μία δυαδική τιμή (αληθές ή ψευδές) που χαρακτηρίζει κάθε επέκταση. Η ύπαρξη της τιμής «αληθές» καθιστά την επέκταση κρίσιμη (critical) ενώ η ύπαρξη της τιμής «ψευδές» καθιστά την επέκταση μη κρίσιμη (non critical). Σε πολλά πρότυπα κάποιες επεκτάσεις χαρακτηρίζονται υποχρεωτικά ως κρίσιμες. Όταν μια επέκταση έχει χαρακτηριστεί κρίσιμη, είναι υποχρεωτικό για την εφαρμογή που χρησιμοποιεί το πιστοποιητικό να μπορεί να την καταλάβει και να την επεξεργαστεί, διαφορετικά το πιστοποιητικό απορρίπτεται. Μια μη κρίσιμη επέκταση μπορεί να επεξεργαστεί μόνο όταν αυτό είναι δυνατόν, αλλιώς μπορεί να αγνοηθεί αν η εφαρμογή που χρησιμοποιεί το πιστοποιητικό δεν την υποστηρίζει. Οι επεκτάσεις ενός πιστοποιητικού X.509v3 περιγράφονται στη συνέχεια.
- Digital Signature: περιέχει την ψηφιακή υπογραφή του πιστοποιητικού καθώς και περιγραφή του κρυπτογραφικού αλγορίθμου που χρησιμοποιήθηκε για τη δημιουργία της.

6.3.3.1 Τύποι Επεκτάσεων Πιστοποιητικών

Όπως είδαμε οι επεκτάσεις προσδίδουν σε ένα πιστοποιητικό επιπρόσθετες πληροφορίες. Οι επεκτάσεις αυτές σύμφωνα με το RFC3280 μπορούν να είναι:

- Επεκτάσεις προσδιορισμού ιδιοκτήτη και εκδότη του πιστοποιητικού (subject and issuer identification extensions).
- Επεκτάσεις ιδιοτήτων του κλειδιού (key attribute extensions).
- Επεκτάσεις πολιτικής (policy extensions).
- Επεκτάσεις περιορισμού μονοπατιού πιστοποίησης (certification path constraints extensions).

- Ιδιωτικές επεκτάσεις Διαδικτύου (private Internet extensions).

Επεκτάσεις προσδιορισμού ιδιοκτήτη και εκδότη του πιστοποιητικού (subject and issuer identification extensions)

Οι επεκτάσεις αυτές χρησιμοποιούνται με σκοπό τον καθορισμό εναλλακτικών διακριτικών ονομασιών για τον ιδιοκτήτη ή τον εκδότη του πιστοποιητικού υποστηρίζοντας έτσι τις απαιτήσεις για ανωνυμία και πολυγλωσσία. Επίσης οι επεκτάσεις αυτές προσφέρουν επιπλέον πληροφορίες για τον ιδιοκτήτη ενός πιστοποιητικού, πέρα από το όνομα του.

- Subject Alternative Name: περιλαμβάνει διαφορετικές μορφές ονομάτων που μπορούν να χαρακτηρίζουν τον ιδιοκτήτη του πιστοποιητικού (π.χ. διεύθυνση ηλεκτρονικού ταχυδρομείου, διεύθυνση IP κλπ).
- Issuer Alternative Name: περιλαμβάνει διαφορετικές μορφές ονομάτων που μπορούν να χαρακτηρίζουν τον εκδότη του πιστοποιητικού (π.χ. διεύθυνση ηλεκτρονικού ταχυδρομείου, διεύθυνση IP κλπ).
- Subject Directory Attributes: συνδέει τον ιδιοκτήτη του πιστοποιητικού με μία σειρά χαρακτηριστικών που τον προσδιορίζουν (π.χ. η εθνικότητα). Αν και η επέκταση αυτή δεν χρησιμοποιείται συχνά, υπάρχουν πολλές γνωστές εφαρμογές στις οποίες η επέκταση αυτή περιέχει πληροφορίες για τα δικαιώματα πρόσβασης του χρήστη στο πιστοποιητικό.

Επεκτάσεις ιδιοτήτων του κλειδιού (key attribute extensions)

Οι επεκτάσεις αυτές δίνουν πληροφορίες σχετικά με τα κλειδιά που ανήκουν σε ένα περιβάλλον PKI και θέτουν περιορισμούς στη χρήση του ζεύγους κλειδιών που αντιστοιχούν στο πιστοποιητικό.

- Authority Key Identifier: η επέκταση αυτή παρέχει ένα τρόπο προσδιορισμού του δημοσίου κλειδιού που ανταποκρίνεται στο ιδιωτικό κλειδί με το οποίο ο εκδότης έχει υπογράψει το πιστοποιητικό. Η επέκταση αυτή χρησιμοποιείται στην περίπτωση που ο εκδότης του πιστοποιητικού έχει περισσότερα του ενός κλειδιά για να υπογράφει τα πιστοποιητικά. Σύμφωνα με το RFC3280 η συμπλήρωση του πεδίου αυτού είναι υποχρεωτική για όλα τα πιστοποιητικά έκτος από τα αυτό-υπογεγραμμένα πιστοποιητικά (self-signed certificates).
- Subject Key Identifier: η επέκταση αυτή παρέχει ένα τρόπο προσδιορισμού των πιστοποιητικών εκείνων που περιέχουν ένα συγκεκριμένο δημόσιο κλειδί. Χρησιμεύει στην περίπτωση που ο ιδιοκτήτης του πιστοποιητικού έχει στην κατοχή του περισσότερα του ενός ζεύγη κλειδιών. Σύμφωνα με το RFC3280 η επέκταση αυτή είναι μη κρίσιμη και προτείνεται στις περιπτώσεις πιστοποιητικών τελικής οντότητας.
- Key Usage: η επέκταση αυτή προσδιορίζει τις λειτουργίες ή τις υπηρεσίες που μπορεί να υποστηρίξει το δημόσιο κλειδί που περιέχεται στο πιστοποιητικό. Για παράδειγμα, το δημόσιο κλειδί του πιστοποιητικού μπορεί να χρησιμοποιηθεί για υποστήριξη υπηρεσιών όπως η ψηφιακή υπογραφή, η μη

αποκήρυξη, η κρυπτογράφηση κλειδιού, η κρυπτογράφηση δεδομένων, η συμφωνία κλειδιού (key agreement), η ψηφιακή υπογραφή πιστοποιητικών, η ψηφιακή υπογραφή Λιστών Ανάκλησης Πιστοποιητικών (Certification Revocation Lists-CRL), η κρυπτογράφηση μόνο (encipher only) και η αποκρυπτογράφηση μόνο (decipher only). Σύμφωνα με το RFC3280 η επέκταση αυτή είναι κρίσιμη.

- Extended Key Usage: η επέκταση αυτή προσδιορίζει μία ή περισσότερες λειτουργίες στις οποίες μπορεί να χρησιμοποιηθεί το δημόσιο κλειδί που περιέχεται στο πιστοποιητικό, επί πρόσθετα ή σε αντικατάσταση των λειτουργιών και υπηρεσιών που αναφέρονται στην επέκταση Key Usage. Τέτοιες λειτουργίες μπορούν να είναι η πιστοποίηση αυθεντικότητας TLS (Transport Layer Security) εξυπηρετητή, η πιστοποίηση αυθεντικότητας TLS πελάτη, ψηφιακή υπογραφή κώδικα (code signing), προστασία ηλεκτρονικού ταχυδρομείου, χρονοσφράγιση (time stamping), και υπογραφή OCSP (Online Certificate Status Protocol). Σύμφωνα με το RFC3280 η επέκταση αυτή χρησιμοποιείται κυρίως σε πιστοποιητικά τελικής οντότητας
- Private Key Usage Period: η επέκταση αυτή χρησιμοποιείται από τον εκδότη του πιστοποιητικού για να προσδιορίσει μια διαφορετική χρονική περίοδο ισχύος του ιδιωτικού κλειδιού από αυτήν του αντίστοιχου δημόσιου κλειδιού που περιέχεται στο πιστοποιητικό. Η επέκταση αυτή είναι πολύ χρήσιμη σε περιπτώσεις δημοσίων κλειδιών που χρησιμοποιούνται για επαλήθευση ψηφιακών υπογραφών. Μία σωστή χρήση της επέκτασης βοηθάει στη μείωση πολλών περιπτώσεων στις οποίες απόλυτα έγκυρες ψηφιακές υπογραφές δεν μπορούν να επαληθευτούν γιατί το ιδιωτικό κλειδί που τις δημιούργησε έχει λήξει.

Επεκτάσεις πολιτικής (policy extensions)

Παρέχουν στους χρήστες τις πληροφορίες που είναι απαραίτητες για να εντοπίσουν και να ανακτήσουν τις πολιτικές σύμφωνα με τις οποίες εκδίδεται και χρησιμοποιείται το πιστοποιητικό.
Επίσης, περιέχουν αναφορές σε πολιτικές άλλων Αρχών Πιστοποίησης που θεωρούνται ισοδύναμες με τις πολιτικές της οικείας Αρχής Πιστοποίησης.
Συναντώνται στις περιπτώσεις διαγώνιας πιστοποίησης (cross certification), έτσι ώστε να διευκολύνεται η λειτουργικότητα στις περιπτώσεις που υπάρχουν συναλλαγές μεταξύ χρηστών που ανήκουν σε διαφορετικά περιβάλλοντα PKI και κατά συνέπεια ακολουθούν διαφορετικές πολιτικές πιστοποίησης.

- Certificate Policies: στην επέκταση αυτή ο εκδότης του πιστοποιητικού μπορεί να συμπεριλάβει τις πολιτικές με βάση τις οποίες εκδίδονται τα πιστοποιητικά. Πρόκειται για πληροφορίες οι οποίες καθορίζουν την ισχύ αλλά και τη χρήση του πιστοποιητικού κάτω από διαφορετικές συνθήκες.
- Policy Mappings: η επέκταση αυτή χρησιμοποιείται μόνο για CA πιστοποιητικά και αφορά συστήματα στα οποία συμμετέχουν περισσότερες από μια Αρχές Έκδοσης Πιστοποιητικών. Η επέκταση αυτή καθορίζει μία

λίστα πολιτικών που εφαρμόζονται από την Αρχή Έκδοσης του πιστοποιητικού, οι οποίες μπορούν να γίνουν αποδεκτές από μία άλλη Αρχή Έκδοσης.

Επεκτάσεις περιορισμού μονοπατιού πιστοποίησης (certification path constraints extensions)

Θέτουν περιορισμούς στον αριθμό των κόμβων που διασχίζονται μέχρι την εμπιστευόμενη Αρχή Έκδοσης, κατά τη διαδρομή πιστοποίησης σε ένα πιστοποιητικό. Με άλλα λόγια περιορίζεται η ανεξέλεγκτη μεταβατικότητα της εμπιστοσύνης σε σχήματα ιεραρχίας ή διαγώνιας πιστοποίησης.

- Basic Constraints: η επέκταση αυτή αποτελείται από δύο πεδία. Το πεδίο CA του οποίου η τιμή (αληθής ή ψευδής) καθορίζει αν το πιστοποιητικό είναι ένα CA πιστοποιητικό και το πεδίο Path Length Constraint το οποίο καθορίζει το μέγιστο αριθμό CA πιστοποιητικών που μπορούν να ακολουθούν το πιστοποιητικό σε ένα μονοπάτι πιστοποίησης. Μια μηδενική τιμή για το πεδίο Path Length Constraint δηλώνει ότι η CA δεν μπορεί να εκδίδει CA πιστοποιητικά αλλά μόνο πιστοποιητικά τελικής οντότητας.
- Name Constraints: η επέκταση αυτή αφορά μόνο CA πιστοποιητικά. Προσδιορίζει ένα χώρο ονομάτων μέσα στον οποίο περιέχονται όλα τα ονόματα των ιδιοκτητών στους οποίους ανήκουν τα πιστοποιητικά ενός μονοπατιού πιστοποίησης.
- Policy Constraints: η επέκταση αυτή υπάρχει μόνο στα CA πιστοποιητικά. Μπορεί να χρησιμοποιηθεί από την CA είτε για να εμποδίσει τη σύγκριση πολιτικών είτε για να εξασφαλίσει ότι κάθε πιστοποιητικό σε ένα μονοπάτι περιέχει μια αποδεκτή πολιτική.
- Inhibit Any Policy: υπάρχει μόνο σε πιστοποιητικά CA και αποκλείει την αποδοχή του αναγνωριστικού πολιτικής anyPolicy από άλλες πολιτικές πιστοποιητικών.

Επεκτάσεις Λιστών Ανάκλησης Πιστοποιητικών

Πρόκειται για επεκτάσεις οι οποίες δίνουν πληροφορίες σχετικά με τα σημεία διανομής Λιστών Ανάκλησης Πιστοποιητικών και διαφορικών Λιστών Ανάκλησης Πιστοποιητικών (deltaCRLs) .

- CRL Distribution Point: η επέκταση αυτή προσδιορίζει το κομμάτι εκείνο της Λίστας Ανάκλησης Πιστοποιητικών στο οποίο βρίσκονται πληροφορίες σχετικά με την ανάκληση του συγκεκριμένου πιστοποιητικού.
- Freshest CRL Pointer (Delta CRL Distribution Point): πρόκειται για μια επέκταση που συναντιέται τόσο σε CA πιστοποιητικά όσο και σε πιστοποιητικά τελικής οντότητας. Προσδιορίζει τον τρόπο με τον οποίο μπορούν να αποκτηθούν πληροφορίες σχετικά με τις διαφορικές ΛΑΠ, παρέχοντας ένα δείκτη στην πιο πρόσφατα ενημερωμένη διαφορική Λίστα Ανάκλησης Πιστοποιητικών.

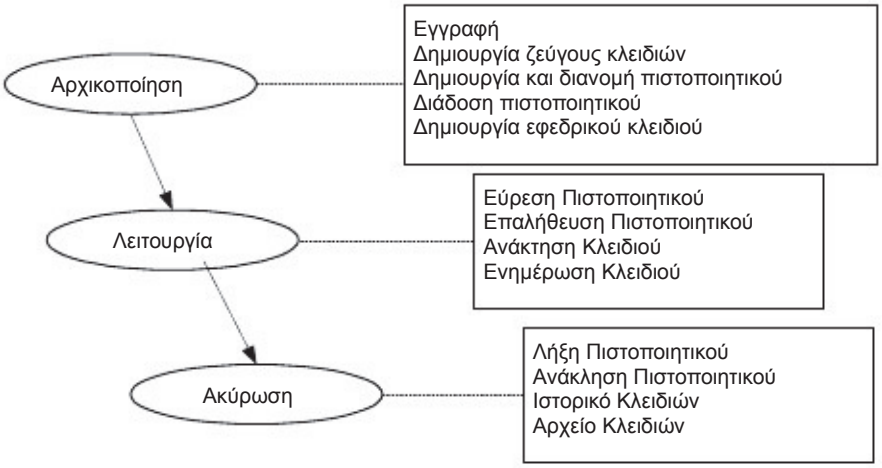
Ιδιωτικές επεκτάσεις Διαδικτύου (Private Internet Extensions)

Πρόκειται για δύο επεκτάσεις που χρησιμοποιούνται σε εφαρμογές Υποδομής Δημοσίου Κλειδιού στο Διαδίκτυο. Οι εφαρμογές αυτές μπορούν, κάνοντας χρήση των συγκεκριμένων επεκτάσεων, να αποκτήσουν on-line πληροφορίες σχετικά με την Αρχή Έκδοσης ή τον ιδιοκτήτη του πιστοποιητικού

- Authority Information Access: εμφανίζεται τόσο σε πιστοποιητικά CA όσο και σε πιστοποιητικά τελικών οντοτήτων. Προσδιορίζει τον τρόπο με τον οποίο μπορεί να γίνει χρήση των πληροφοριών και των υπηρεσιών που προσφέρει ο εκδότης του πιστοποιητικού. Στις πληροφορίες και τις υπηρεσίες περιλαμβάνονται μεταξύ άλλων υπηρεσίες on-line ελέγχου εγκυρότητας πιστοποιητικών και πληροφορίες πολιτικής της Αρχής Έκδοσης.
- Subject Information Access : εμφανίζεται τόσο σε πιστοποιητικά CA όσο και σε πιστοποιητικά τελικών οντοτήτων και προσδιορίζει πώς μπορούν να υλοποιηθούν πληροφορίες και υπηρεσίες που προσφέρονται από τον ιδιοκτήτη του πιστοποιητικού. Τέτοιες πληροφορίες και υπηρεσίες μπορούν να είναι ο προσδιορισμός της θέσης της αποθήκης πιστοποιητικών και οι Λίστες Ανάκλησης Πιστοποιητικών στην περίπτωση που ο ιδιοκτήτης του πιστοποιητικού είναι μια Αρχή Έκδοσης και η υπηρεσία χρονοσφράγισης στην περίπτωση που ο ιδιοκτήτης είναι μια τελική οντότητα.

6.4 Διαχείριση Κλειδιών και Πιστοποιητικών (Key and Certificate Management)

Στο κεφάλαιο αυτό θα αναφερθούμε στις διάφορες φάσεις λειτουργίας κατά τη διάρκεια του κύκλου ζωής ενός ζεύγους κλειδιών και ενός πιστοποιητικού. Το σχήμα 6.2 δείχνει τις τρεις φάσεις του κύκλου ζωής ενός κλειδιού και ενός πιστοποιητικού, τη φάση αρχικοποίησης, τη φάση ισχύος και τη φάση ακύρωσης.



Σχήμα 6.2: Κύκλος ζωής πιστοποιητικών/ κλειδιών

6.4.1 Φάση Αρχικοποίησης

Στη φάση αρχικοποίησης λαμβάνουν χώρα όλες οι απαραίτητες διαδικασίες που θα πρέπει να ολοκληρωθούν πριν την εισαγωγή μιας οντότητας σε ένα περιβάλλον PKI.

6.4.1.1 Εγγραφή

Κατά τη διαδικασία της εγγραφής επαληθεύεται η ταυτότητα ενός χρήστη ο οποίος έχει κάνει αίτηση για απόκτηση ενός ψηφιακού πιστοποιητικού. Η επαλήθευση της ταυτότητας του πελάτη είναι συνήθως μια διαδικασία που απαιτεί τη φυσική παρουσία του πελάτη και στην οποία χρησιμοποιούνται επίσημα έγγραφα που πιστοποιούν ότι ο πελάτης είναι πράγματι αυτός που ισχυρίζεται ότι είναι (π.χ μια ταυτότητα).

6.4.1.2 Δημιουργία ζεύγους κλειδιών

Στο στάδιο αυτό δημιουργείται ένα ζεύγος δημόσιου και ιδιωτικού κλειδιού με χρήση ενός κατάλληλου κρυπτογραφικού αλγορίθμου. Το δημόσιο και το ιδιωτικό κλειδί μπορούν να δημιουργηθούν είτε στο περιβάλλον του χρήστη, είτε μέσα σε μία Αρχή Πιστοποίησης είτε μέσα σε μία Αρχή Καταχώρησης. Το πού θα δημιουργηθούν τελικά τα κλειδιά εξαρτάται από παράγοντες όπως η απόδοση, η ασφάλεια και η προσδοκώμενη χρήση των κλειδιών. Γενικά σε περιπτώσεις που είναι επιθυμητή η μη αποκήρυξη προτείνεται το ζεύγος κλειδιών να δημιουργείται από την πλευρά του χρήστη. Σε περίπτωση που το ζεύγος κλειδιών δημιουργηθεί σε μία τρίτη αρχή, π.χ. την Αρχή Πιστοποίησης, αυτή αναλαμβάνει και την ασφαλή μεταφορά του ιδιωτικού κλειδιού στον ιδιοκτήτη του.

6.4.1.3 Δημιουργία και διανομή πιστοποιητικού

Ανεξαρτήτως του πού έχει δημιουργηθεί ένα ζεύγος κλειδιών, η δημιουργία ενός ψηφιακού πιστοποιητικού αποτελεί μοναδική ευθύνη μιας εξουσιοδοτημένης Αρχής Πιστοποίησης. Στην περίπτωση που το δημόσιο κλειδί έχει δημιουργηθεί από την πλευρά του χρήστη, τότε αυτό πρέπει να μεταφερθεί με ασφάλεια στην Αρχή Πιστοποίησης ώστε να τοποθετηθεί στο πιστοποιητικό. Από τη στιγμή που το πιστοποιητικό έχει δημιουργηθεί θα πρέπει να διανεμηθεί με ασφάλεια. Ο τρόπος με τον οποίον θα διανεμηθούν τα πιστοποιητικά εξαρτάται από διάφορους παράγοντες όπως η προσδοκώμενη χρήση του πιστοποιητικού ή τυχόν περιορισμοί πολιτικών. Για παράδειγμα, ένα πιστοποιητικό από τη στιγμή που θα εκδοθεί μπορεί να διανεμηθεί απευθείας στον ιδιοκτήτη ή σε ένα απομακρυσμένο κατάλογο πιστοποιητικών ή και τα δύο. Ένα πλήθος πρωτοκόλλων ορίζουν ένα ασφαλές περιβάλλον μέσα στο οποίο μπορούν να διανεμηθούν με ασφάλεια τα πιστοποιητικά. Τα πρωτόκολλα αυτά είναι τα: CMP , CRMF , PKCS#7 , PKCS#10 , CMC , SCEP

6.4.1.4 Διάδοση πιστοποιητικού

Από τη στιγμή που ένα ψηφιακό πιστοποιητικό εκδίδεται και φτάνει με ασφάλεια στον ιδιοκτήτη του, θα πρέπει να μοιραστεί και στις υπόλοιπες οντότητες για να το χρησιμοποιήσουν. Πιθανές μέθοδοι για τη διάδοση του πιστοποιητικού περιλαμβάνουν:

- Διάδοση του πιστοποιητικού χωρίς τη χρήση ηλεκτρονικών τεχνικών (π.χ με το ταχυδρομείο)
- Δημοσίευση του πιστοποιητικού σε κοινά προσβάσιμους καταλόγους (LDAP) ή βάσεις δεδομένων.
- Διάδοση του πιστοποιητικού με χρήση ασφαλούς ηλεκτρονικού ταχυδρομείου

6.4.1.5 Δημιουργία εφεδρικού κλειδιού

Όπως έχει ήδη αναφερθεί η δημιουργία ενός εφεδρικού κλειδιού είναι πολύ σημαντική σε περίπτωση που το αρχικό ιδιωτικό κλειδί χαθεί ή καταστραφεί. Με αυτόν τον τρόπο, για παράδειγμα, μία επιχείρηση θα μπορεί να συνεχίζει να αποκρυπτογραφεί δεδομένα που την αφορούν χωρίς να χρειάζεται να αποκτήσει νέο κλειδί. Συνήθως η δημιουργία του εφεδρικού κλειδιού λαμβάνει χώρα κατά τη δημιουργία του αρχικού ζεύγος κλειδιών. Το σημείο αποθήκευσης των εφεδρικών κλειδιών μπορεί να είναι είτε η ίδια η Αρχή Πιστοποίησης που εκδίδει τα αντίστοιχα πιστοποιητικά, είτε κάποια ανεξάρτητη αρχή.

6.4.2 Φάση Λειτουργίας

Στη φάση αυτή λαμβάνουν χώρα όλες εκείνες οι διαδικασίες που αφορούν στη σωστή χρήση κλειδιών και πιστοποιητικών σε ένα περιβάλλον PKI, μετά τη δημιουργία και ασφαλή διανομή τους.

6.4.2.1 Εύρεση Πιστοποιητικού

Το δημόσιο κλειδί που βρίσκεται μέσα σε ένα πιστοποιητικό μπορεί να χρησιμοποιηθεί από μια οντότητα είτε για την κρυπτογράφηση δεδομένων που προορίζονται για τον ιδιοκτήτη του πιστοποιητικού είτε για την επαλήθευση της ψηφιακής υπογραφής του. Είναι λοιπόν σημαντικό να μπορεί ο καθένας να βρει εύκολα το πιστοποιητικό που αναζητά μέσα σε μία δομή δεδομένων που περιέχει όλα τα πιστοποιητικά.

6.4.2.1 Επαλήθευση Πιστοποιητικού

Από τη στιγμή της εύρεσης ενός πιστοποιητικού είναι σημαντικό να γίνεται και επαλήθευση της ακεραιότητας του, που σημαίνει ότι, η οντότητα που κάνει χρήση του πιστοποιητικού θα πρέπει να είναι σίγουρη ότι το περιεχόμενό του δεν έχει αλλοιωθεί. Επειδή κάθε πιστοποιητικό που εκδίδεται υπογράφεται ψηφιακά από την αρχή πιστοποίησης, η επαλήθευση του πιστοποιητικού, και άρα ο έλεγχος της

ακεραιότητας του, επιτυγχάνεται με την επαλήθευση της ψηφιακής υπογραφής της αρχής πιστοποίησης.

6.4.2.2 Ανάκτηση κλειδιού

Επειδή η απώλεια του ιδιωτικού κλειδιού από κάποιους χρήστες είναι αναπόφευκτη κρίνεται απαραίτητο από μια ολοκληρωμένη Υποδομή Δημοσίου Κλειδιού να διαθέτει μηχανισμούς ανάκτησης των χαμένων κλειδιών. Ένας τέτοιος μηχανισμός ανάκτησης είναι η δημιουργία εφεδρικών κλειδιών από την Αρχή Πιστοποίησης ή από ανεξάρτητες έμπιστες αρχές.

6.4.2.3 Ενημέρωση Κλειδιού

Όπως έχει ήδη αναφερθεί τα πιστοποιητικά έχουν ένα συγκεκριμένο χρόνο ζωής από τη στιγμή που εκδίδονται. Όταν ένα πιστοποιητικό πλησιάζει στην ημερομηνία λήξης του θα πρέπει να εκδίδεται ένα νέο ιδιωτικό κλειδί και το αντίστοιχο πιστοποιητικό του. Η διαδικασία αυτή ονομάζεται ενημέρωση κλειδιού. Η ενημέρωση κλειδιού είναι πολύ σημαντική και σε ένα ολοκληρωμένο σύστημα PKI θα πρέπει να γίνεται αυτόματα, αφού δεν είναι πάντα εύκολο για τον ιδιοκτήτη του πιστοποιητικού να θυμάται την ημερομηνία λήξης του, ειδικά όταν έχει στην κατοχή του περισσότερα του ενός πιστοποιητικά.

6.4.3 Φάση Ακύρωσης

Πρόκειται για την τελευταία φάση που περιλαμβάνει ό,τι έχει να κάνει με το τέλος του κύκλου ζωής των κλειδιών και των πιστοποιητικών.

6.4.3.1 Λήξη Πιστοποιητικού

Πρόκειται για τη φυσική διαδικασία λήξης του πιστοποιητικού από τη στιγμή που αυτό ξεπεράσει την χρονική περίοδο ισχύος του. Αφού το πιστοποιητικό λήξει μπορεί να ανανεωθεί, οπότε το ίδιο δημόσιο κλειδί τοποθετείται σε ένα νέο πιστοποιητικό με νέα περίοδο ισχύος. Υπάρχει επίσης η δυνατότητα έκδοσης ενός νέου ζεύγους κλειδιών και άρα ενός νέου πιστοποιητικού, όπως επίσης και η δυνατότητα να μη γίνει καμία ενέργεια. Στην τελευταία αυτή περίπτωση ο τελικός χρήστης παύει να ανήκει στη συγκεκριμένη Υποδομή Δημοσίου Κλειδιού.

6.4.3.2 Ανάκληση Πιστοποιητικού

Όπως έχει ήδη αναφερθεί, πολλές φορές κρίνεται απαραίτητη η ακύρωση ενός ψηφιακού πιστοποιητικού πριν την καθορισμένη ημερομηνία λήξης του. Σε κάποιες περιπτώσεις μπορεί να χρειαστεί ο ίδιος ο χρήστης να διακόψει την ισχύ του πιστοποιητικού του, οπότε θα πρέπει με κάποιο τρόπο, ηλεκτρονικό ή μη, να ενημερώσει την αρμόδια αρχή πιστοποίησης ή καταχώρησης γι' αυτό. Επίσης, η ανάκληση πιστοποιητικών μπορεί να γίνεται και από αρμόδιους διαχειριστές όταν

αυτό κρίνεται απαραίτητο.

6.4.3.3 Ιστορικό Κλειδιών

Στο ιστορικό κλειδιών αποθηκεύονται τα κλειδιά εκείνα, των οποίων το αντίστοιχο πιστοποιητικό έχει λήξει. Συνήθως πρόκειται για ιδιωτικά κλειδιά που χρησιμοποιούνται για αποκρυπτογράφηση δεδομένων και αποθηκεύονται προκειμένου να διασφαλιστεί ότι τα δεδομένα που έχουν κρυπτογραφηθεί με τα αντίστοιχα δημόσια κλειδιά θα συνεχίζουν να αποκρυπτογραφούνται ακόμα και μετά τη λήξη του πιστοποιητικού τους.

6.4.3.4 Αρχείο Κλειδιών

Πρόκειται για μια μακροπρόθεσμη αποθήκευση κλειδιών και πιστοποιητικών που συνήθως υποστηρίζεται από μία αρχή πιστοποίησης ή κάποια άλλη έμπιστη αρχή. Το Αρχείο Κλειδιών διαφέρει από το ιστορικό κλειδιών ως προς το ότι το περιεχόμενο του πρώτου χρησιμοποιείται για ελεγκτικούς σκοπούς καθώς και για επίλυση διαφωνιών που έχουν να κάνουν με παραποίηση της ακεραιότητας δεδομένων, αποκήρυξη συγκεκριμένης ενέργειας κ.α.

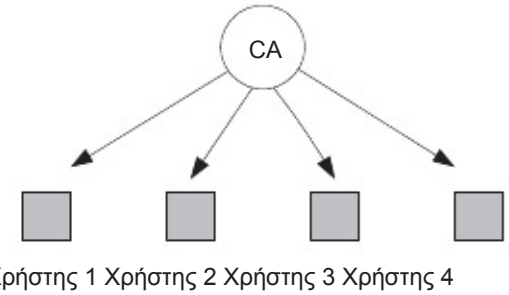
6.5 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΥΠΟΔΟΜΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Η τεχνολογία της Υποδομής Δημοσίου Κλειδιού χρησιμοποιείται σήμερα από πολλούς οργανισμούς και επιχειρήσεις ως ένα εργαλείο διασφάλισης ευαίσθητων εταιρικών πόρων. Επειδή όμως κάθε επιχείρηση έχει τις δικές τις ανάγκες και απαιτήσεις καθίσταται φανερό ότι η ύπαρξη ενός καθολικού μοντέλου μιας ΥΔΚ δεν είναι εφικτή. Για το λόγο αυτό υπάρχουν διάφορες αρχιτεκτονικές ΥΔΚ που εξυπηρετούν τις διαφορετικές ανάγκες κάθε οργανισμού. Παρά τις διαφορές που παρουσιάζουν μεταξύ τους, ο πυρήνας και ο πρωταρχικός στόχος κάθε αρχιτεκτονικής ΥΔΚ είναι η ασφάλεια των ηλεκτρονικών συναλλαγών που λαμβάνουν χώρα σε αυτή.

6.5.1 Αρχιτεκτονική Υποδομής Δημοσίου Κλειδιού με μοναδική Αρχή Πιστοποίησης (Single CA Architecture)

Πρόκειται για τον πιο βασικό τύπο αρχιτεκτονικής Υποδομής Δημοσίου Κλειδιού. Σε αυτήν την αρχιτεκτονική υπάρχει μόνο μια Αρχή Πιστοποίησης (CA) η οποία εκδίδει και διανέμει τα πιστοποιητικά και τις Λίστες Ανάκλησης Πιστοποιητικών. Κάθε χρήστης με τη σειρά του εμπιστεύεται την αρχή πιστοποίησης και χρησιμοποιεί μόνο πιστοποιητικά που εκδίδονται από αυτήν. Εξ ορισμού, η αρχιτεκτονική με μοναδική Αρχή Πιστοποίησης δεν μπορεί να επεκταθεί και να συμπεριλάβει και άλλες αρχές πιστοποίησης δημιουργώντας έτσι δυσκολία σε θέματα κλιμάκωσης. Αυτό το είδος αρχιτεκτονικής είναι κατάλληλο για μικρούς οργανισμούς με περιορισμένο αριθμό χρηστών, δημιουργεί όμως προβλήματα στην περίπτωση αύξησης των χρηστών

εξαιτίας της αδυναμίας της να συμπεριλάβει και άλλες Αρχές Πιστοποίησης.
Το σχήμα 6.3 παρουσιάζει το μοντέλο μιας αρχιτεκτονικής με μοναδική Αρχή Πιστοποίησης.

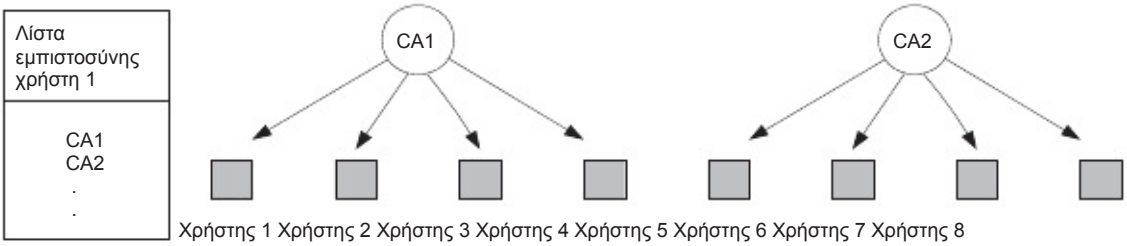


Σχήμα 6.3: PKI με μοναδική αρχή πιστοποίησης

Όλες οι οντότητες επικοινωνούν μεταξύ τους έχοντας ως κοινό σημείο εμπιστοσύνης την CA. Έτσι κάθε μια από τις οντότητες εμπιστεύεται αυτομάτως τα πιστοποιητικά των υπολοίπων.
Η υλοποίηση μιας αρχιτεκτονικής με μοναδική αρχή πιστοποίησης είναι σχετικά απλή αφού απαιτείται μόνο μία CA. Ταυτόχρονα όμως η ύπαρξη μιας μόνο αρχής πιστοποίησης αποτελεί και το μεγαλύτερο μειονέκτημα της αρχιτεκτονικής˙ στην περίπτωση που χαθεί το ιδιωτικό κλειδί της CA ακυρώνονται όλα τα πιστοποιητικά που έχουν εκδοθεί από αυτή, γεγονός που μπορεί να οδηγήσει στην ολική κατάρρευση του συστήματος PKI.

6.5.1.1 Βασικό μοντέλο λιστών εμπιστοσύνης (Basic Trust List Model)

Το μοντέλο Λιστών Εμπιστοσύνης αποτελεί τον πιο απλό εμπλουτισμό της αρχιτεκτονικής με μοναδική Αρχή Πιστοποίησης. Στο μοντέλο αυτό οι υπηρεσίες ενός PKI προσφέρονται από έναν αριθμό αρχών πιστοποίησης ανάμεσα στις οποίες όμως δεν αναπτύσσονται σχέσεις εμπιστοσύνης. Οι χρήστες ενός τέτοιου μοντέλου θα πρέπει να διατηρούν μια λίστα των αρχών πιστοποίησης που εμπιστεύονται και να χρησιμοποιούν μόνο πιστοποιητικά και Λίστες Ανάκλησης Πιστοποιητικών που έχουν εκδοθεί από τις Αρχές Πιστοποίησης που περιέχονται σε αυτή τη λίστα. Μια νέα Αρχή Πιστοποίησης μπορεί να προστεθεί στη υποδομή PKI με τροποποίηση της λίστας εμπιστοσύνης. Το μοντέλο λιστών εμπιστοσύνης είναι αυτό που χρησιμοποιείται από τους χρήστες Διαδικτύου για την επίτευξη συνδέσεων με εξυπηρετητές web.



Σχήμα 6.4: Βασικό μοντέλο Λιστών Εμπιστοσύνης

Στην περίπτωση του σχήματος 6.4 για να μπορέσουν να επικοινωνήσουν ο χρήστης 1 με το χρήστη 5 θα πρέπει ο χρήστης 1 να έχει στην λίστα του την CA2 στην οποία ανήκει ο χρήστης 5 και από τη μεριά του ο χρήστης 5 να έχει στη λίστα του τη CA1 στην οποία ανήκει ο χρήστης 1. Παρόλο που το μοντέλο αυτό είναι αρκετά απλό στο σχεδιασμό του, μπορεί να γίνει αρκετά πολύπλοκο σε κάποιες περιπτώσεις. Για παράδειγμα, είναι πολύ πιθανό ένας χρήστης να προσθέσει στη λίστα του μια Αρχή Πιστοποίησης χωρίς να την ενημερώσει για αυτό. Σε περίπτωση που το ιδιωτικό κλειδί αυτής της Αρχής Πιστοποίησης χαθεί, τότε δε θα είναι σε θέση να ειδοποιήσει αυτόν τον χρήστη ότι δεν μπορεί πλέον να εμπιστεύεται τα πιστοποιητικά που έχει εκδώσει. Επίσης σε ένα τέτοιο μοντέλο, καθώς αυξάνεται ο αριθμός των Αρχών Πιστοποίησης που εμπιστεύεται μία οντότητα, αυξάνεται και ο αριθμός των εισόδων στη λίστα εμπιστοσύνης της. Έτσι κάθε οντότητα έχει στην κατοχή της ένα πλήθος σημαντικών πληροφοριών που αφορούν τις εμπιστευόμενες Αρχές Πιστοποίησης. Η διατήρηση αλλά και η ενημέρωση αυτών των πληροφοριών από τους χρήστες είναι συχνά μια δύσκολη υπόθεση καθώς ο αριθμός των Αρχών Πιστοποίησης αυξάνεται.

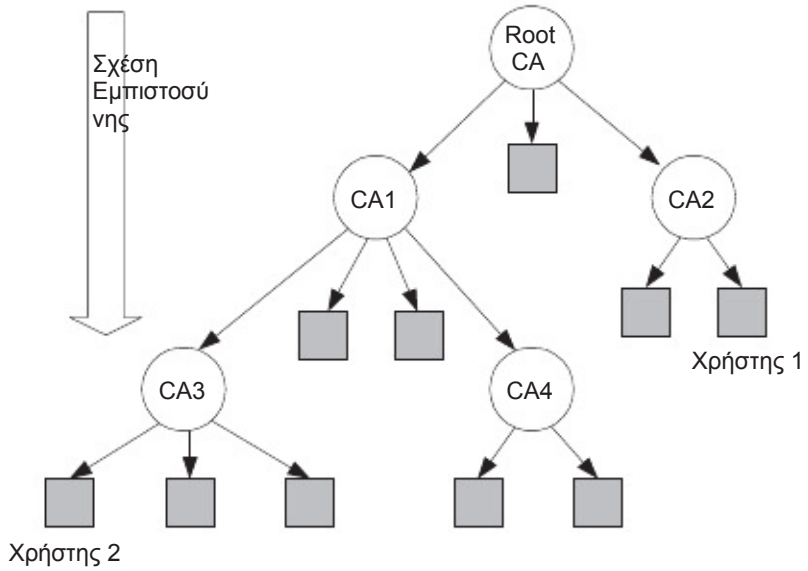
6.5.2 Επιχειρηματική αρχιτεκτονική Υποδομής Δημοσίου Κλειδιού (Enterprise PKI Architecture)

Στην ενότητα αυτή θα παρουσιαστούν δύο μοντέλα αρχιτεκτονικής, το ιεραρχικό μοντέλο και η αρχιτεκτονική πλέγματος, που χρησιμοποιούνται από επιχειρήσεις και οργανισμούς των οποίων την κλίμακα δεν μπορεί να εξυπηρετήσει η απλή αρχιτεκτονική μοναδικής Αρχής Πιστοποίησης. Και το δύο αυτά μοντέλα βασίζονται στην ύπαρξη πολλαπλών Αρχών Πιστοποίησης κατάλληλα συνδυασμένων, έτσι ώστε να ικανοποιούν τις ανάγκες του εκάστοτε περιβάλλοντος.

6.5.2.1 Ιεραρχική αρχιτεκτονική Υποδομής Δημοσίου Κλειδιού (Hierarchical PKI)

Σε αυτήν την αρχιτεκτονική PKI υπάρχουν πολλαπλές Αρχές Πιστοποίησης ανάμεσα στις οποίες έχουν αναπτυχθεί σχέσεις εμπιστοσύνης. Η δομή αυτής της αρχιτεκτονικής παραπέμπει σε ένα ανεστραμμένο δέντρο, στην κορυφή του οποίου βρίσκεται η Αρχή Πιστοποίησης ρίζας (root CA). Κάτω από την Αρχή Πιστοποίησης ρίζας βρίσκονται υφιστάμενες Αρχές Πιστοποίησης. Η ριζική Αρχή Πιστοποίησης συνήθως εκδίδει πιστοποιητικά για τις υφιστάμενες Αρχές Πιστοποίησης και όχι για τους χρήστες. Οι υφιστάμενες Αρχές Πιστοποίησης μπορούν να εκδώσουν πιστοποιητικά τόσο για τους χρήστες όσο και για της υφιστάμενες Αρχές Πιστοποίησης που βρίσκονται σε χαμηλότερο επίπεδο στην ιεραρχία. Στο ιεραρχικό PKI, οι υφιστάμενες Αρχές Πιστοποίησης δεν μπορούν να εκδώσουν πιστοποιητικά για τις προϊστάμενες Αρχές Πιστοποίησης και τη ριζική Αρχή Πιστοποίησης. Εκτός από την ριζική Αρχή Πιστοποίησης, όλες οι υπόλοιπες αρχές έχουν μία μοναδική προϊστάμενη Αρχή Πιστοποίησης. Για να προστεθεί μια καινούρια Αρχή

Πιστοποίησης στο μοντέλο, η ριζική αρχή ή οποιαδήποτε άλλη προϊστάμενη Αρχή εκδίδει ένα πιστοποιητικό στην καινούρια Αρχή Πιστοποίησης.
Το σχήμα 6.5 βοηθά στο να κατανοήσουμε καλύτερα την Ιεραρχική αρχιτεκτονική PKI.



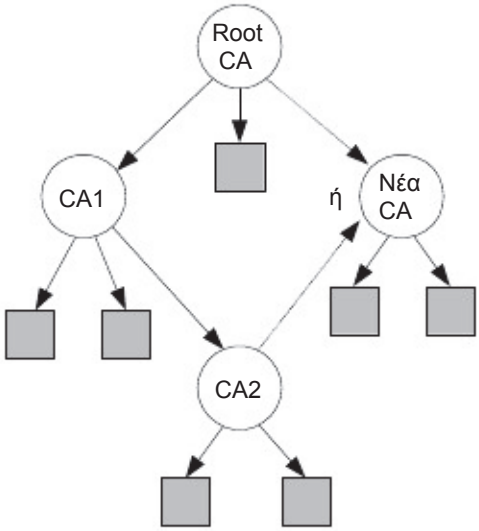
Σχήμα 6.5: Ιεραρχικό μοντέλο PKI

Η ριζική Αρχή Πιστοποίησης εκδίδει πιστοποιητικά για τις αμέσως υφιστάμενες CA1 και CA2 οι οποίες με τη σειρά τους εκδίδουν πιστοποιητικά για τις δικές τους υφιστάμενες αρχές (CA3 και CA4). Οι τελευταίες στην ιεραρχία Αρχές Πιστοποίησης (CA2, CA3 και CA4) εκδίδουν πιστοποιητικά για τις τελικές οντότητες που είναι οι χρήστες του συστήματος. Στο ιεραρχικό μοντέλο, για να εμπιστευτεί ένας χρήστης το πιστοποιητικό ενός άλλου χρήστη, θα πρέπει ο πρώτος να ανακτήσει κάθε πιστοποιητικό ενδιάμεσης Αρχής Πιστοποίησης μεταξύ του άλλου χρήστη και της ρίζας. Με άλλα λόγια θα πρέπει να επαληθεύσει το μονοπάτι πιστοποίησης (certification path) που περνάει από τις ενδιάμεσες Αρχές Πιστοποίησης μέχρι τη ρίζα. Για παράδειγμα: Στο παραπάνω σχήμα για να επικοινωνήσει με ασφάλεια ο Χρήστης 1 με τον Χρήστη 2 θα πρέπει ο Χρήστης 1 να επαληθεύσει το πιστοποιητικό της CA3, στη συνέχεια το πιστοποιητικό της CA1 φτάνοντας τελικά στην ριζική CA, την οποία εμπιστεύεται. Αντίστοιχα ο Χρήστης2 θα πρέπει να επαληθεύσει το πιστοποιητικό της CA2 και τελικά το πιστοποιητικό της ριζικής CA, την οποία εμπιστεύεται.
Το ιεραρχικό μοντέλο PKI παρουσιάζει τέσσερις βασικές ιδιότητες που οφείλονται στην απλή δομή του και στη μονή κατεύθυνση της σχέσης εμπιστοσύνης ανάμεσα στις αρχές πιστοποίησης :

- Εύκολη επεκτασιμότητα: για να δημιουργηθεί μια σχέση εμπιστοσύνης με μία νέα αρχή πιστοποίησης το μόνο που απαιτείται είναι είτε η ριζική αρχή να αποκτήσει σχέση εμπιστοσύνης με την νέα αρχή πιστοποίησης είτε μία υφιστάμενη αρχή πιστοποίησης.(Σχήμα 6.6)
- Μικρό μονοπάτι πιστοποίησης: οι διαδρομές πιστοποίησης σε μία ιεραρχική δομή PKI είναι μικρές. Η μεγαλύτερη διαδρομή είναι ίση με το βάθος του δέντρου συν ένα, δηλαδή το πιστοποιητικό CA για κάθε υφιστάμενη αρχή

πιστοποίησης συν το πιστοποιητικό του χρήστη.

- Οι διαδρομές από το πιστοποιητικό ως τη ρίζα είναι εύκολα αναγνωρίσιμες.
- Τα πιστοποιητικά είναι μικρότερα από αυτά που αναπτύσσονται στην αρχιτεκτονική πλέγματος PKI.



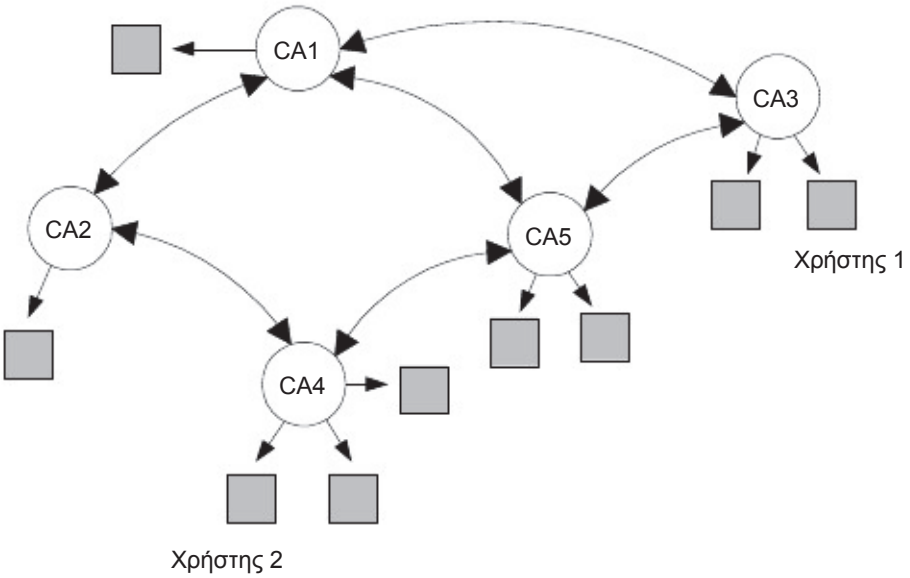
Σχήμα 6.6: Προσθήκη νέας CA στο ιεραρχικό μοντέλο PKI

Παρόλα τα πλεονεκτήματα, στο ιεραρχικό μοντέλο PKI υπάρχει το μεγάλο μειονέκτημα της ύπαρξης ενός μοναδικού σημείου εμπιστοσύνης, της ριζικής Αρχής Πιστοποίησης. Στην περίπτωση που η ρίζα δεχθεί πλήγμα τότε θα καταρρεύσει όλο το οικοδόμημα του PKI που στηρίζεται σε αυτή. Άλλο σημαντικό μειονέκτημα είναι ότι στο ανταγωνιστικό περιβάλλον στο οποίο αναπτύσσονται οι εταιρίες, είναι δύσκολο να επιτευχθεί συμφωνία για το ποια θα είναι η ριζική Αρχή Πιστοποίησης. Επίσης, σημαντικό μειονέκτημα είναι το σημαντικό κόστος μετάβασης από το μοντέλο μοναδικής Αρχής Πιστοποίησης στο μοντέλο ιεραρχικής δομής PKI αφού όλοι οι χρήστες που ανήκουν σε ένα PKI μοναδικής Αρχής Πιστοποίησης θα πρέπει να αλλάξουν το σημείο εμπιστοσύνης τους τοποθετώντας το στη ριζική αρχή. Η πρόταση για να ξεπεραστούν τα προβλήματα του ιεραρχικού μοντέλου είναι η αρχιτεκτονική πλέγματος PKI.

6.5.2.2 Αρχιτεκτονική πλέγματος Υποδομής Δημοσίου Κλειδιού (Mesh PKI)

Στην αρχιτεκτονική πλέγματος PKI, οι πολλαπλές Αρχές Πιστοποίησης συνδέονται μεταξύ τους μία σχέση ομότιμη προς ομότιμη (peer to peer relationship). Στην αρχιτεκτονική αυτή όλες οι Αρχές Πιστοποίησης μπορούν να θεωρηθούν σημεία εμπιστοσύνης. Οι Αρχές Πιστοποίησης μπορούν να εκδίδουν πιστοποιητικά όχι μόνο για τους τελικούς χρήστες αλλά και η μία για την άλλη με αποτέλεσμα να μοιράζονται μία αμφίδρομη σχέση εμπιστοσύνης. Σε μία αρχιτεκτονική πλέγματος PKI όλες οι Αρχές Πιστοποίησης πρέπει να πιστοποιούνται μεταξύ τους. Όπως έχει ήδη αναφερθεί η διαδικασία πιστοποίησης ανάμεσα σε δύο Αρχές Πιστοποίησης ονομάζεται διαγώνια πιστοποίηση (cross certification). Κατά τη διαγώνια

πιστοποίηση εδραιώνεται μία αμοιβαία σχέση εμπιστοσύνης ανάμεσα στις δύο αρχές πιστοποίησης. Η διαγώνια πιστοποίηση λαμβάνει χώρα κάθε φορά που δύο χρήστες που ανήκουν σε διαφορετικές αρχές θέλουν να επικοινωνήσουν μεταξύ τους. Επειδή στο μοντέλο πλέγματος PKI υπάρχουν πολλαπλά σημεία εμπιστοσύνης, μια ενδεχόμενη απώλεια εμπιστοσύνης μίας Αρχής Πιστοποίησης δεν μπορεί να οδηγήσει σε κατάρρευση ολόκληρου του PKI. Επίσης η είσοδος μιας νέας Αρχής Πιστοποίησης στο μοντέλο είναι εύκολη, αφού το μόνο που χρειάζεται είναι οι υπάρχουσες Αρχές Πιστοποίησης να εκδώσουν ένα πιστοποιητικό για τη νέα Αρχή Πιστοποίησης. Το σχήμα 6.7 βοηθάει στην καλύτερη κατανόηση της αρχιτεκτονικής πλέγματος PKI.



Σχήμα 6.7: Αρχιτεκτονική Πλέγματος Υποδομής Δημοσίου Κλειδιού

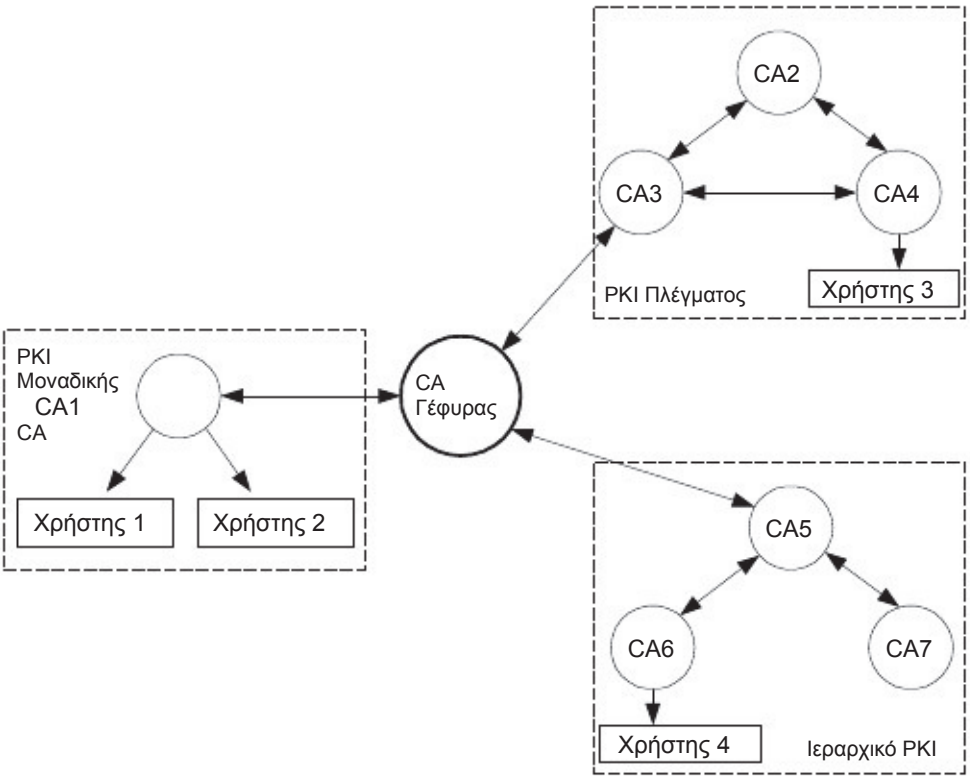
Ο Χρήστης 1 γνωρίζει το δημόσιο κλειδί της CA3 και ο Χρήστης 2 γνωρίζει το δημόσιο κλειδί της CA4. Υπάρχουν πολλά μονοπάτια πιστοποίησης που οδηγούν από τον Χρήστη 1 στο Χρήστη 2. Το συντομότερο απαιτεί από τον Χρήστη 1 να επαληθεύσει το πιστοποιητικό του Χρήστη 2, το οποίο εκδόθηκε από την CA4, στη συνέχεια να επαληθεύσει το πιστοποιητικό της CA4 που εκδόθηκε από την CA5 και τελικά να επαληθεύσει το πιστοποιητικό της CA5 που εκδόθηκε από την CA3. Η CA3 είναι η CA του Χρήστη 1 την οποία εμπιστεύεται και γνωρίζει το δημόσιο κλειδί της.

6.5.3 Υβριδική αρχιτεκτονική Υποδομής Δημοσίου Κλειδιού (Hybrid PKI architecture)

Οι υβριδικές αρχιτεκτονικές PKI δημιουργήθηκαν για να εξυπηρετήσουν την ανάγκη επικοινωνίας ανάμεσα σε δύο ή περισσότερα περιβάλλοντα που χρησιμοποιούν διαφορετικές μορφές αρχιτεκτονικής PKI. Το σημαντικότερο μοντέλο υβριδικής αρχιτεκτονικής PKI είναι αυτό της αρχιτεκτονικής Αρχής Πιστοποίησης τύπου γέφυρας (Bridge CA architecture) το οποίο θα μελετηθεί αναλυτικά παρακάτω.

6.5.3.1 Αρχιτεκτονική Αρχής Πιστοποίησης τύπου γέφυρας (Bridge CA architecture)

Η αρχιτεκτονική Αρχής Πιστοποίησης τύπου γέφυρας σχεδιάστηκε για να συνδέει συστήματα Υποδομών Δημοσίου Κλειδιού ανεξαρτήτως των αρχιτεκτονικών που χρησιμοποιούν. Η ιδέα βασίζεται στην ύπαρξη μίας νέας Αρχής Πιστοποίησης, που ονομάζεται Αρχή Πιστοποίησης γέφυρας (bridge CA), της οποίας μοναδικός σκοπός είναι η δημιουργία σχέσεων εμπιστοσύνης ανάμεσα σε διαφορετικά περιβάλλοντα PKI. Οι σχέσεις αυτές συνδυάζονται με τέτοιο τρόπο ώστε οι οντότητες να επικοινωνούν μεταξύ τους μόνο μέσω της Αρχής Πιστοποίησης γέφυρας.
Αντίθετα με μία Αρχή Πιστοποίησης που ανήκει σε μία αρχιτεκτονική πλέγματος, η Αρχή Πιστοποίησης γέφυρας δεν μπορεί να εκδώσει πιστοποιητικά απευθείας στους χρήστες. Επίσης, αντίθετα με την ριζική Αρχή Πιστοποίησης, η Αρχή Πιστοποίησης γέφυρας δεν χρησιμοποιείται ως το μοναδικό σημείο εμπιστοσύνης. Όλοι οι χρήστες μιας τέτοιας αρχιτεκτονικής PKI θεωρούν την Αρχή Πιστοποίησης γέφυρας ένα μεσολαβητή που δημιουργεί σχέσεις τύπου ομότιμη προς ομότιμη μεταξύ διαφορετικών PKI.
Στην περίπτωση που μία ιεραρχική δομή λαμβάνει μέρος σε μία αρχιτεκτονική τύπου γέφυρας, η Αρχή Πιστοποίησης γέφυρας θα αναπτύξει σχέση εμπιστοσύνης με την ριζική Αρχή Πιστοποίησης. Αν στην αρχιτεκτονική τύπου γέφυρας λαμβάνει χώρα ένα PKI τύπου πλέγματος, η Αρχή Πιστοποίησης γέφυρας θα αναπτύξει σχέση εμπιστοσύνης με μία από τις Αρχές Πιστοποίησης. Το σχήμα 6.8 βοηθάει στην καλύτερη κατανόηση της αρχιτεκτονικής πλέγματος



Σχήμα 6.8: Αρχιτεκτονική Υποδομής Δημοσίου Κλειδιού με CA Γέφυρας

Στο σχήμα 6.8 η Αρχή Πιστοποίησης γέφυρας έχει αναπτύξει σχέσεις με τρεις τύπους αρχιτεκτονικών PKI. Η πρώτη είναι μια μοναδική Αρχή Πιστοποίησης του Χρήστη 1 και του Χρήστη 2, η δεύτερη είναι μία ιεραρχική δομή PKI του Χρήστη 3 και η τρίτη είναι μία δομή πλέγματος PKI του Χρήστη 4. Κανένας από τους χρήστες δεν εμπιστεύεται άμεσα την Αρχή Πιστοποίησης γέφυρας. Ο Χρήστης 1 και ο Χρήστης 2 εμπιστεύονται την CA1 που εξέδωσε τα πιστοποιητικά τους˙ εμπιστεύονται και την Αρχή Πιστοποίησης γέφυρας γιατί η CA1 εξέδωσε ένα πιστοποιητικό για αυτήν. Το σημείο εμπιστοσύνης του Χρήστη 4 είναι η ριζική Αρχή Πιστοποίησης της ιεραρχίας της (δηλ. η CA5) ˙ εμπιστεύεται την Αρχή Πιστοποίησης γέφυρας γιατί η ριζική Αρχή Πιστοποίησης εξέδωσε ένα πιστοποιητικό για αυτήν. Ο Χρήστης 3 εμπιστεύεται εκείνη την Αρχή Πιστοποίησης του πλέγματος που εξέδωσε το δικό του πιστοποιητικό (δηλ. τη CA3) ˙ εμπιστεύεται επίσης την Αρχή Πιστοποίησης γέφυρας γιατί υπάρχει ένα έγκυρο μονοπάτι πιστοποίησης από την Αρχή Πιστοποίησης που εξέδωσε το δικό του πιστοποιητικό στην Αρχή Πιστοποίησης γέφυρας. Ο Χρήστης 1 ή ο Χρήστης 2 μπορούν να χρησιμοποιήσουν τη γέφυρα εμπιστοσύνης που υπάρχει μέσω της Αρχή Πιστοποίησης γέφυρας για να επικοινωνήσουν με τον Χρήστη 3 και τον Χρήστη 4.

6.6 ΥΠΗΡΕΣΙΕΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (PKI Services)

6.6.1 Ανάκληση Πιστοποιητικού (Certificate Revocation)

Πολλές φορές κρίνεται απαραίτητη η ακύρωση ενός ψηφιακού πιστοποιητικού πριν την καθορισμένη ημερομηνία λήξης του. Υπάρχουν διάφοροι λόγοι που θα μπορούσαν να οδηγήσουν στην ακύρωση ενός πιστοποιητικού, όπως για παράδειγμα:

- Διαρροή του ιδιωτικού κλειδιού του κατόχου του πιστοποιητικού.
- Αλλαγή των πληροφοριών που χαρακτηρίζουν την οντότητα, όπως για παράδειγμα αλλαγή επωνύμου.
- Διαρροή του ιδιωτικού κλειδιού της Αρχής Πιστοποίησης.

Όταν λοιπόν για οποιοδήποτε λόγο κριθεί απαραίτητη η ακύρωση του πιστοποιητικού ενός χρήστη του δικτύου, θα πρέπει να υπάρχει ένας μηχανισμός που να ειδοποιεί τους υπόλοιπους ότι δεν μπορούν πλέον να χρησιμοποιούν το δημόσιο κλειδί αυτής της οντότητας. Αυτόν τον μηχανισμό εξυπηρετεί η υπηρεσία δημοσίου κλειδιού που ονομάζεται Ανάκληση Πιστοποιητικού (Certificate Revocation). Σε περιπτώσεις ανάκλησης πιστοποιητικού η Αρχή Καταχώρησης (RA) θα πρέπει να ενημερώσει την Αρχή Πιστοποίησης για το ποια πιστοποιητικά θα πρέπει να ακυρωθούν.
Οι μηχανισμοί που χρησιμοποιούνται από την Αρχή Πιστοποίησης για το σκοπό αυτό είναι:

- Περιοδικοί Μηχανισμοί Δημοσίευσης (Periodic Publication Mechanisms): ο μηχανισμός αυτός περιλαμβάνει τη χρήση λιστών ανάκλησης πιστοποιητικών (Certificate Revocation Lists-CRL) και τη χρήση δέντρων ανάκλησης πιστοποιητικών (Certificate Revocation Trees-CRT). Μία λίστα ανάκλησης

πιστοποιητικών (CRL) είναι μία υπογεγραμμένη λίστα που περιέχει τα πιστοποιητικά που έχουν ανακληθεί. Η λίστα αυτή μπορεί να ανανεώνεται κάθε 1 ως 24 ώρες. Το δέντρο ανάκλησης πιστοποιητικών (CRT) βασίζεται στα δέντρα κατακερματισμού Merkle. Στην περίπτωση ενός CRT, το δέντρο περιέχει όλες τις γνωστές πληροφορίες που αφορούν ανακληθέντα πιστοποιητικά μέσα σε ένα γνωστό σύνολο δικτύων PKI.

- Online Μηχανισμοί Αναζήτησης (Online Query Mechanisms): ο μηχανισμός αυτός προσφέρει στο σύστημα πραγματικού χρόνου ενημέρωση ως προς τα πιστοποιητικά που έχουν ανακληθεί. Αυτού του είδους ο μηχανισμός είναι κατάλληλος για συναλλαγές υψηλής προτεραιότητας, όπως για παράδειγμα οι οικονομικές συναλλαγές. Στην περίπτωση της ενημέρωση πραγματικού χρόνου γίνεται χρήση του πρωτοκόλλου OCSP (Online Certificate Status Protocol) ή των Online Transaction Validation Protocols. Το OCSP [35] ορίζει ένα μηχανισμό ενημέρωσης σχετικά με την εγκυρότητα πιστοποιητικών δημόσιου κλειδιού. Τα Online Transaction Validation Protocols χρησιμοποιούνται για on-line έλεγχο της εγκυρότητας συναλλαγών όπως είναι οι εμπορικές συναλλαγές μέσω πιστωτικής κάρτας.

Θα πρέπει να σημειωθεί ότι υπάρχει μία έμμεση σχέση ανάμεσα στις πληροφορίες που περιέχει ένα πιστοποιητικό και το χρήσιμο χρόνο ζωής του. Χονδρικά ισχύει ο κανόνας όσο πιο πολλές οι πληροφορίες σε ένα πιστοποιητικό, τόσο μικρότερη η χρησιμότητά του. Αυτό συμβαίνει γιατί είναι πολύ πιθανό οι πληροφορίες που περιέχονται στο πιστοποιητικό να αλλάξουν. Έτσι ένα παλιό πιστοποιητικό μπορεί να ανακληθεί και ένα νέο πιστοποιητικό να εκδοθεί πριν τη λήξη του προηγούμενου. Ένα από τα πιο σημαντικά ζητήματα στο θέμα της ανάκλησης των πιστοποιητικών είναι η συχνότητα με την οποία οι πληροφορίες της ανάκλησης ανανεώνονται και δημοσιεύονται. Αν οι χρήστες δεν ενημερωθούν έγκαιρα για την ακύρωση κάποιου πιστοποιητικού μπορεί να εμπιστευθούν ένα άκυρο πιστοποιητικό. Η καθυστέρηση μεταξύ του χρόνου που η Αρχή Πιστοποίησης λαμβάνει την πληροφορία ότι ένα πιστοποιητικό πρέπει να ανακληθεί και του χρόνου που τελικά η Αρχή Πιστοποίησης ανακοινώνει και δημοσιεύει την ανάκληση ονομάζεται καθυστέρηση ανάκλησης (revocation delay), Η καθυστέρηση ανάκλησης θα πρέπει να είναι όσο το δυνατόν μικρότερη και θα πρέπει να προσδιορίζεται στην πολιτική των πιστοποιητικών (certificate policy). Η πολιτική των πιστοποιητικών είναι ένα έγγραφο που προσδιορίζει την πολιτική ασφαλείας κατά την διαχείριση των πιστοποιητικών. Η σύνταξη ενός τέτοιου εγγράφου είναι αρμοδιότητα της Αρχή Πιστοποίησης.

6.6.2 Δημιουργία εφεδρικού κλειδιού και ανάκτηση κλειδιού (Key backup and recovery)

Σε ένα περιβάλλον Υποδομής Δημοσίου Κλειδιού υπάρχουν πολλοί λόγοι που μπορούν να οδηγήσουν στην απώλεια του ιδιωτικού κλειδιού ενός ή περισσοτέρων χρηστών. Τέτοιοι λόγοι μπορεί να είναι η απώλεια ενός κωδικού που ξεκλειδώνει το κωδικοποιημένο ιδιωτικό κλειδί, η καταστροφή ή η αντικατάσταση ενός αποθηκευτικού μέσου (π.χ ενός σκληρού δίσκου ή μιας έξυπνης κάρτας) που περιέχει το ιδιωτικό κλειδί κ.α. Η απώλεια τέτοιου είδους δεδομένων μπορεί να αποβεί καταστροφική. Η λύση στο πρόβλημα της απώλειας ενός ιδιωτικού κλειδιού δίνεται

με την δημιουργία εφεδρικού κλειδιού και ανάκτηση κλειδιού (key backup and recovery). Το εφεδρικό κλειδί είναι στην ουσία ένα αντίγραφο ασφαλείας του ιδιωτικού κλειδιού και συνήθως δημιουργείται από την Αρχή Πιστοποίησης κατά την δημιουργία του πιστοποιητικού. Ας σημειωθεί ότι η δημιουργία εφεδρικού κλειδιού δεν είναι απαραίτητη στην περίπτωση που το κλειδί χρησιμοποιείται για ψηφιακή υπογραφή.

6.6.3 Αυτόματη ανανέωση κλειδιού (Automatic Key Update)

Κάθε πιστοποιητικό από την στιγμή της έκδοσης του έχει περιορισμένη διάρκεια ζωής. Καθώς το πιστοποιητικό πλησιάζει στη λήξη του, θα πρέπει να δημιουργηθεί ένα νέο ζεύγος δημοσίου και ιδιωτικού κλειδιού καθώς και ένα νέο πιστοποιητικό. Η διαδικασία αυτή είναι γνωστή ως ανανέωση κλειδιού (key update). Οι περισσότεροι χρήστες ενός δικτύου όμως δεν μπορούν να θυμούνται την ημερομηνία λήξης των πιστοποιητικών τους με αποτέλεσμα να μην τα ανανεώνουν έγκαιρα. Το πρόβλημα αυτό μπορεί να ξεπεραστεί αν η ανανέωση του κλειδιού γίνεται αυτόματα από την ίδια την Υποδομή Δημοσίου Κλειδιού και χωρίς την παρέμβαση κάποιου χρήστη. Η διαδικασία αυτή ονομάζεται αυτόματη ανανέωση κλειδιού (Automatic Key Update). Κάθε φορά που ένα πιστοποιητικό χρησιμοποιείται, ελέγχεται η περίοδος ισχύος του. Στην περίπτωση που πλησιάζει η ημερομηνία λήξης του δημιουργείται ένα νέο πιστοποιητικό που αντικαθιστά το παλιό. Τα νέα κλειδιά χρησιμοποιούνται για τις μελλοντικές διαδικασίες ψηφιακής υπογραφής και κρυπτογράφησης. Το παλιό πιστοποιητικό διατηρείται σε περίπτωση που χρειαστεί για επαλήθευση ψηφιακής υπογραφής και αποκρυπτογράφηση δεδομένων με το παλιό ιδιωτικό κλειδί.

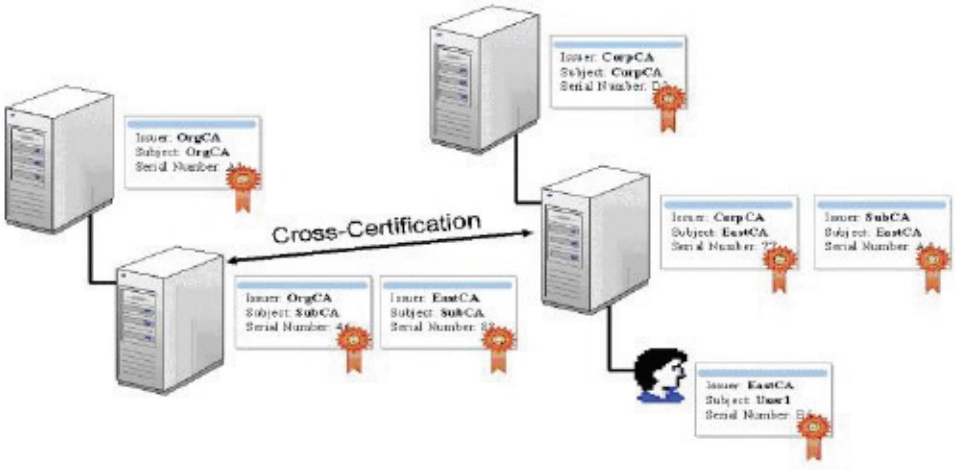
6.6.4 Ιστορικό κλειδιών (Key history)

Είδαμε παραπάνω ότι καθώς ένα πιστοποιητικό πλησιάζει την ημερομηνία λήξης του, αντικαθίσταται από ένα καινούριο που περιέχει νέα κλειδιά κρυπτογράφησης. Αυτό δε σημαίνει ότι τα δεδομένα που κρυπτογραφήθηκαν με τα παλιά κλειδιά δε θα μπορούν πλέον να ανακτηθούν. Για αυτό το λόγο είναι σημαντική η ασφαλής αποθήκευση των παλιών ιδιωτικών κλειδιών ακόμη και αν το πιστοποιητικό τους έχει λήξει. Η αποθήκευση των παλιών κλειδιών έχει ως αποτέλεσμα την δημιουργία ενός ιστορικού κλειδιών (key history), στο οποίο μπορεί εύκολα να ανατρέξει ο χρήστης όποτε χρειαστεί. Οι πληροφορίες του ιστορικού κλειδιών συνήθως αποθηκεύονται τοπικά στο χρήστη, μπορούν όμως να αποθηκευτούν και στην Αρχή Πιστοποίησης ή σε κάποια έμπιστη αρχή, εφόσον βέβαια είναι δυνατή η ασφαλής ανάκτηση τους.

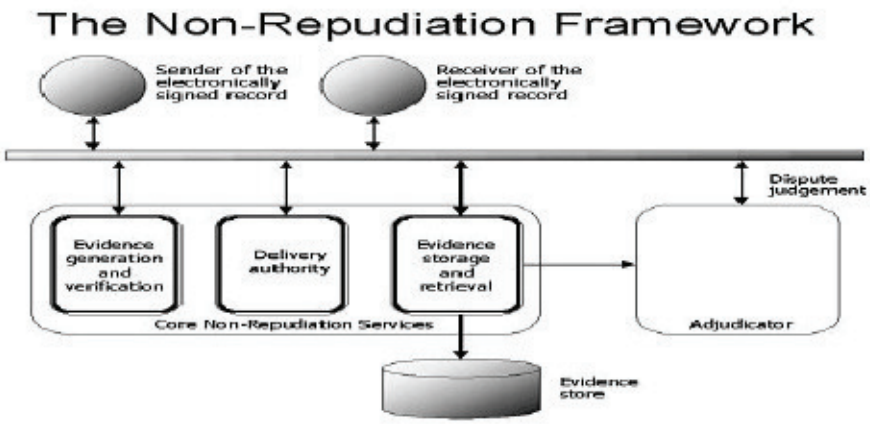
6.6.5 Δια-πιστοποίηση (Cross certification)

Η δια-πιστοποίηση είναι ένας χρήσιμος μηχανισμός για την δημιουργία μιας αμφίδρομης σχέσης εμπιστοσύνης μεταξύ δύο Αρχών Πιστοποίησης. Κατά τη διαδικασία της δια-πιστοποίησης συγκρίνονται οι πολιτικές ασφαλείας και οι πρακτικές που εφαρμόζει κάθε αρχή και αν βρεθούν κοινά σημεία τότε κάθε μία αρχή εκδίδει ένα πιστοποιητικό για την άλλη. Η δια-πιστοποίηση χρησιμοποιείται για να

επεκτείνει τις σχέσεις εμπιστοσύνης ανάμεσα σε περιβάλλοντα Υποδομής Δημοσίου Κλειδιού που αρχικά ήταν ασύνδετα μεταξύ τους.



6.6.6 Μη αποκήρυξη (non-repudiation)

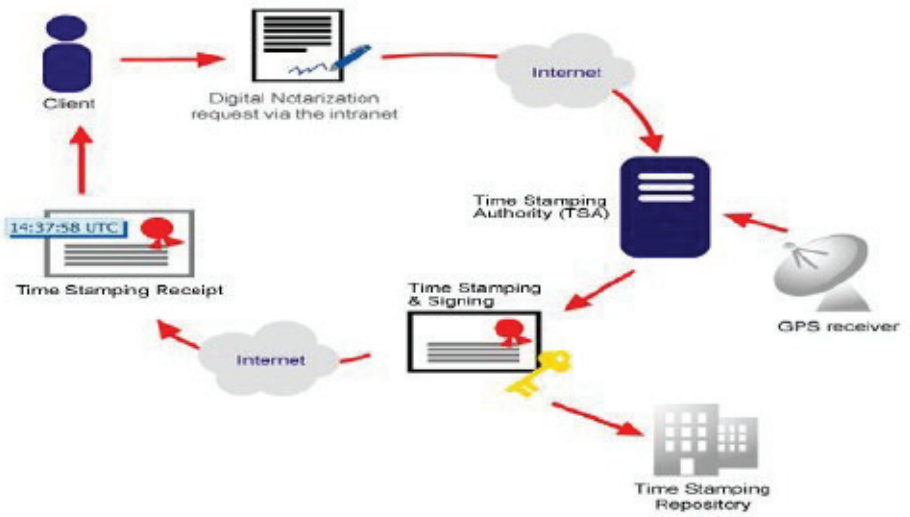


Μη αποκήρυξη είναι η υπηρεσία εκείνη που διασφαλίζει ότι μία οντότητα δε θα μπορεί να αρνηθεί μελλοντικά τη συμμετοχή της σε κάποια δράση. Η βασική ιδέα είναι ότι η οντότητα δεσμεύεται κρυπτογραφικά με κάθε συγκεκριμένη πράξη, με τέτοιο τρόπο, ώστε πιθανή άρνησή της να αποτελεί παραδοχή αμέλειας ή κακεντρέχειας. Τέτοια πράξη μπορεί να είναι κάποια οικονομική συναλλαγή στο Διαδίκτυο, η δημιουργία και η αποστολή ή λήψη ενός εγγράφου κ.α. Έτσι συχνά γίνεται λόγος για μη αποκήρυξη της προέλευσης, της παραλαβής, και της αποδοχής. Η μη αποκήρυξη είναι από τις πιο σημαντικές αλλά ταυτόχρονα και πιο πολύπλοκες υπηρεσίες μιας Υποδομής Δημοσίου κλειδιού. Η σωστή λειτουργία της βασίζεται στην ύπαρξη και άλλων υπηρεσιών όπως είναι η ασφαλής χρονοσφράγιση και η ασφαλής συμβολαιογραφία. Σημαντική είναι επίσης και η δυνατότητα ασφαλούς αποθήκευσης πληροφοριών χρήσιμων για την επίλυση διαφωνιών, όπως είναι ψηφιακά πιστοποιητικά μετά τα λήξη τους, παλιές λίστες πιστοποιητικών, σφραγίδες

χρόνου κ.α. Σε αυτή την περίπτωση η δυσκολία έγκειται στο να βρεθεί μία ισορροπία ανάμεσα στο πλήθος και το είδος των πληροφοριών που θα αποθηκευτούν και θα θεωρηθούν επαρκής για την επίλυση οποιασδήποτε διαμάχης. Η διατήρηση, λοιπόν, της μη αποκήρυξης σε μία Υποδομή Δημόσιου Κλειδιού είναι πολύπλοκη και επικεντρώνεται στην προστασία του ιδιωτικού κλειδιού. Η μεγαλύτερη αδυναμία ενός συστήματος με Υποδομή Δημοσίου Κλειδιού είναι η ικανότητά του να προστατεύει και να αποδεικνύει ότι έχει στην κατοχή του το ιδιωτικό κλειδί που χρησιμοποιείται για τις ψηφιακές συναλλαγές.

6.6.7 Χρονοσφράγιση (Time stamping)

Μία από τις πιο σημαντικές υπηρεσίες για την υποστήριξη της μη-αποκήρυξης σε μια Υποδομή Δημοσίου Κλειδιού, είναι αυτή της ασφαλούς χρονοσφράγισης (secure time stamping). Η ασφαλής χρονοσφράγιση χρησιμοποιείται για να αποδείξει ότι ένα ορισμένο δεδομένο υπήρξε πριν από κάποια συγκεκριμένη χρονική στιγμή. Κάτι τέτοιο είναι πολύ σημαντικό όταν πρόκειται για δεδομένα που αφορούν οικονομικές ή νομικές συναλλαγές, ιατρικά αρχεία κ.α. Η συσχέτιση μίας πληροφορίας με κάποια συγκεκριμένη χρονική στιγμή γίνεται από μία έμπιστη Τρίτη αρχή, την Αρχή Χρονοσφράγισης (Time Stamping Authority-TSA) . Η τεχνική της δημιουργία μιας σφραγίδας χρόνου (timestamp) βασίζεται στις ψηφιακές υπογραφές και στις συναρτήσεις κατακερματισμού . Ο χρήστης της υπηρεσίας στέλνει στην Αρχή Χρονοσφράγισης ένα αίτημα για ασφαλή χρονοσφράγιση, το οποίο αποτελείται από μια σύνοψη της πληροφορίας. Η σύνοψη της πληροφορίας έχει προκύψει από τη χρήση μιας συνάρτησης κατακερματισμού. Όταν η Αρχή Χρονοσφράγισης λάβει το αίτημα του πελάτη, επισυνάπτει στη σύνοψη της πληροφορίας τον χρόνο στον οποίο την έλαβε. Το μήνυμα που προκύπτει υπογράφεται ψηφιακά με το ιδιωτικό κλειδί της Αρχής Χρονοσφράγισης και αποτελεί πλέον την σφραγίδα χρόνου η οποία αποστέλλεται στον πελάτη .



6.6.8 Συμβολαιογραφία (Notarization)

Η υπηρεσία ασφαλούς ψηφιακής συμβολαιογραφίας είναι για τις ανάγκες μιας Υποδομής Δημοσίου Κλειδιού συνώνυμη με την έννοια της πιστοποίησης δεδομένων. Αυτό σημαίνει ότι η συγκεκριμένη υπηρεσία πιστοποιεί την εγκυρότητα ή την ορθότητα δεδομένων. Για παράδειγμα, ένα ηλεκτρονικό συμβολαιογραφείο μπορεί να θεωρήσει έγκυρη μία ψηφιακή υπογραφή αφού κάνει τους εξής ελέγχους:

- Η υπογραφή επαληθεύεται με τη χρήση του αντίστοιχου δημοσίου κλειδιού
- Το δημόσιο κλειδί ανήκει πράγματι στην οντότητα που ισχυρίζεται ότι έχει δημιουργήσει την ψηφιακή υπογραφή.
- Όλα τα υπόλοιπα στοιχεία που χρειάζονται για την επαλήθευση της υπογραφής (όπως πρόσθετα πιστοποιητικά για τον έλεγχο μονοπατιών πιστοποίησης) είναι διαθέσιμα και αξιόπιστα .

Το συμβολαιογραφείο μιας ΥΔΚ είναι μια οντότητα την οποία εμπιστεύεται ένα σύνολο άλλων οντοτήτων ΥΔΚ ως προς το ότι διεκπεραιώνει σωστά την υπηρεσία συμβολαιογραφίας. Μετά την επαλήθευσή τους, τα δεδομένα υπογράφονται ψηφιακά και χρονοσφραγίζονται.

6.6.9 Διαχείριση προνομίων (Privilege management)

Ο όρος διαχείριση προνομίων είναι ένα γενικός όρος που περιλαμβάνει έννοιες όπως η εξουσιοδότηση, ο έλεγχος πρόσβασης, η διαχείριση δικαιωμάτων, η διαχείριση άδειας κοκ. Η υπηρεσία μέσα από κάποιους κανόνες καθορίζει τι μπορεί και τι δεν μπορεί να κάνει μια οντότητα ή μια ομάδα οντοτήτων μέσα σε ένα συγκεκριμένο περιβάλλον. Η διαχείριση προνομίων δημιουργεί και ενισχύει αυτούς τους κανόνες διατηρώντας με αυτόν τον τρόπο ένα επιθυμητό επίπεδο ασφάλειας.

6.7 ΠΡΟΤΥΠΑ ΥΠΟΔΟΜΗΣ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ (PKI Standards)

Η Διεθνής Επιτροπή Τηλεπικοινωνιών (International Telecommunications Union-ITU) και ο Διεθνής Οργανισμός Προτυποποίησης (International Standards Organization-ISO) έχουν προτείνει μια πληθώρα προτύπων για τον ορισμό πρωτοκόλλων και δομών δεδομένων που αφορούν μία Υποδομή Δημοσίου Κλειδιού. Στη συνέχεια θα εξεταστούν τα σημαντικότερα από αυτά τα πρότυπα.

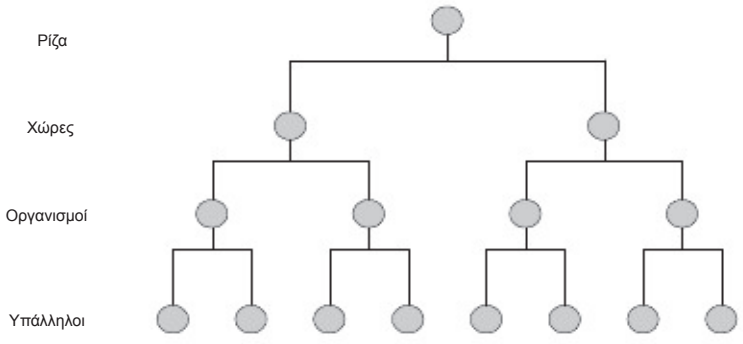
6.7.1 X.509

Το πρότυπο X.509, από τη στιγμή που προτάθηκε, έγινε παγκοσμίως αποδεκτό από όλες τις εφαρμογές που υποστήριζαν και υλοποιούσαν μία Υποδομή Δημοσίου Κλειδιού. Το πρότυπο αυτό περιγράφει ένα ιεραρχικό μοντέλο διαγώνιας πιστοποίησης πιστοποιητικών που προέρχονται από διαφορετικές Αρχές Πιστοποίησης. Τα πιστοποιητικά X.509 πιστοποιούν την αυθεντικότητα μιας οντότητας αποθηκεύοντας πληροφορίες και προνόμια που την αφορούν με τη μορφή χαρακτηριστικών (attributes) μέσα στο πιστοποιητικό. Το πρότυπο X.509

υποστηρίζεται από έναν αριθμό πρωτοκόλλων όπως τα πρωτόκολλα PEM, PKCS, και S-HTTP..

6.7.2 X.500

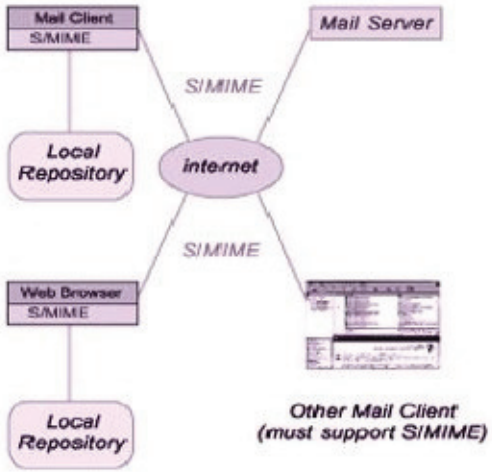
Το πρότυπο X.500 δρα ως ηλεκτρονικό ευρετήριο πιστοποιητικών και Λιστών Ανακληθέντων Πιστοποιητικών. Η πρώτη έκδοση του X.500 εμφανίστηκε το 1988. Πρόκειται για μια παγκόσμια υπηρεσία καταλόγου, που σημαίνει ότι οι πληροφορίες ενός οργανισμού μπορούν να αποθηκευτούν τοπικά σε μία ή περισσότερες βάσεις δεδομένων, οι οποίες αναφέρονται ως Παράγοντες Υπηρεσίας Καταλόγου (Directory Service Agents-DSA). Ένας Παράγοντας Υπηρεσίας Καταλόγου δεν είναι μοναδικός για κάθε οργανισμό και μπορεί να περιέχει πληροφορίες από έναν ή περισσότερους οργανισμούς. Επίσης πληροφορίες που αφορούν ένα μεγάλο οργανισμό μπορούν να αποθηκευτούν σε περισσότερα του ενός DSA. Σε ένα ηλεκτρονικό ευρετήριο που ακολουθεί το πρότυπο X.500, η ανταλλαγή πληροφοριών ανάμεσα σε δύο Παράγοντες Υπηρεσίας Καταλόγου γίνεται μέσω μιας ιεραρχικής δομής που καλείται Δένδρο Πληροφορίας Καταλόγου (Directory Information Tree-DIT). Κάθε κόμβος του δέντρου παίρνει ένα Σχετικό Ξεχωριστό Όνομα (Relative Distinguished Name-RDN) και ονομάζεται ακμή (vertex), έχει ένα κατάλογο πατέρα (parent directory) και πολλούς καταλόγους παιδία (children directory) καθένα από τα οποία παίρνει το δικό του RDN. Στην κορυφή ενός Δένδρου Πληροφορίας Καταλόγου βρίσκεται μία ρίζα, κάτω από την οποία υπάρχουν ακμές για όλα τις χώρες του κόσμου. Κάτω από την ακμή κάθε χώρας υπάρχουν ακμές για όλους τους οργανισμούς, υπηρεσίες και επιχειρήσεις αυτής της χώρας και κάτω από τις ακμές των οργανισμών, υπηρεσιών και επιχειρήσεων υπάρχουν ακμές για κάθε υπάλληλο που εργάζονται σε αυτές κοκ μέχρι να φτάσουμε στο τέλος του δέντρου. Στο σχήμα 6 .9 απεικονίζεται η δομή του X.500.



Σχήμα 6.9 : Η οργάνωση του ευρετηρίου X.500

Η μεγάλη χρησιμότητα του X.500 έγκειται στο ότι είναι τεχνικά επιτεύξιμη η σύνδεση εξυπηρετητών καταλόγων που ανήκουν σε ανεξάρτητα περιβάλλοντα PKI, επιτρέποντας έτσι μια ασφαλή επικοινωνία σε παγκόσμια κλίμακα.

6.7.3 Secure Multipurpose Internet Mail Extension (S/MIME)



Η ανταλλαγή ηλεκτρονικών μηνυμάτων μέσω του Διαδικτύου αποτελεί στις μέρες μας ένα από τους πιο λειτουργικούς και γρήγορους τρόπους επικοινωνίας. Το ηλεκτρονικό ταχυδρομείο μας επιτρέπει να στέλνουμε μηνύματα τα οποία μπορεί να περιέχουν ευαίσθητα προσωπικά ή εταιρικά δεδομένα. Καθώς τα περισσότερα μηνύματα στέλνονται ως απλό κείμενο χωρίς καμία ιδιαίτερη ασφάλεια, καθίσταται εύκολη η παραποίηση του περιεχομένου τους. Προκειμένου να αντιμετωπίσουν αυτό το πρόβλημα ασφάλειας, οι περισσότερες σημερινές εφαρμογές ηλεκτρονικής αλληλογραφίας βασίζονται σε ένα ανοιχτό πρότυπο, γνωστό ως Secure Multipurpose Internet Mail Extension (S/MIME) .
Τα δύο πιο σημαντικά χαρακτηριστικά ασφαλείας του S/MIME είναι:

- Πιστοποίηση αυθεντικότητας: με τη χρήση ψηφιακών υπογραφών το S/MIME πιστοποιεί την αυθεντικότητα του αποστολέα και του παραλήπτη ενός ηλεκτρονικού μηνύματος.
- Ιδιωτικότητα (privacy) : το S/MIME παρέχει ιδιωτικότητα κρυπτογραφώντας τα ηλεκτρονικά μηνύματα.

Σήμερα το S/MIME βρίσκεται στην τρίτη του έκδοση (S/MIMEv3) . Η S/MIMEv3 παρέχει σε σχέση με τις προηγούμενες εκδόσεις την επιπλέον δυνατότητα να μαρκάρονται τα μηνύματα με ετικέτες ασφαλείας (security labels) ανάλογα με το επίπεδο ασφάλειας τους (π.χ. «απόρρητο», «άκρως απόρρητο» ή «εμπιστευτικό») και τη δυνατότητα αίτησης και λήψης μίας ψηφιακά υπογεγραμμένης απόδειξης (digitally signed receipt) που σημαίνει απόδειξη ότι ο παραλήπτης έλαβε ένα αρχικό μήνυμα. Επίσης, παρέχει ευελιξία ως προς τη χρήση διαφορετικών τεχνικών διαχείρισης κλειδιών (key management flexibility) καθώς και τη δυνατότητα υλοποίησης λιστών ηλεκτρονικού ταχυδρομείου (mailing lists). Στην S/MIMEv3 γίνεται λόγος για χρήση δομών Υποδομής Δημοσίου Κλειδιού όπως τα ψηφιακά πιστοποιητικά και οι Λίστες Ανάκληση Πιστοποιητικών.
Συνολικά τα πλεονεκτήματα χρήσης του S/MIME είναι:

- Αν και χρησιμοποιείται κυρίως για τα ηλεκτρονικά μηνύματα, μπορεί να χρησιμοποιηθεί και σε άλλους μηχανισμούς που μεταφέρουν MIME δεδομένα,

όπως το HTTP.

- Όλες οι εφαρμογές που χρησιμοποιούν το πρότυπο S/MIME παρέχουν τα βασικά χαρακτηριστικά ασφαλείας, όπως μυστικότητα, ακεραιότητα δεδομένων και πιστοποίηση αυθεντικότητας.
- Επιτρέπει την ασφαλή ανταλλαγή μηνυμάτων ακόμη και μεταξύ χρηστών που χρησιμοποιούν διαφορετικές εφαρμογές ηλεκτρονικού ταχυδρομείου.

ΚΕΦΑΛΑΙΟ 7

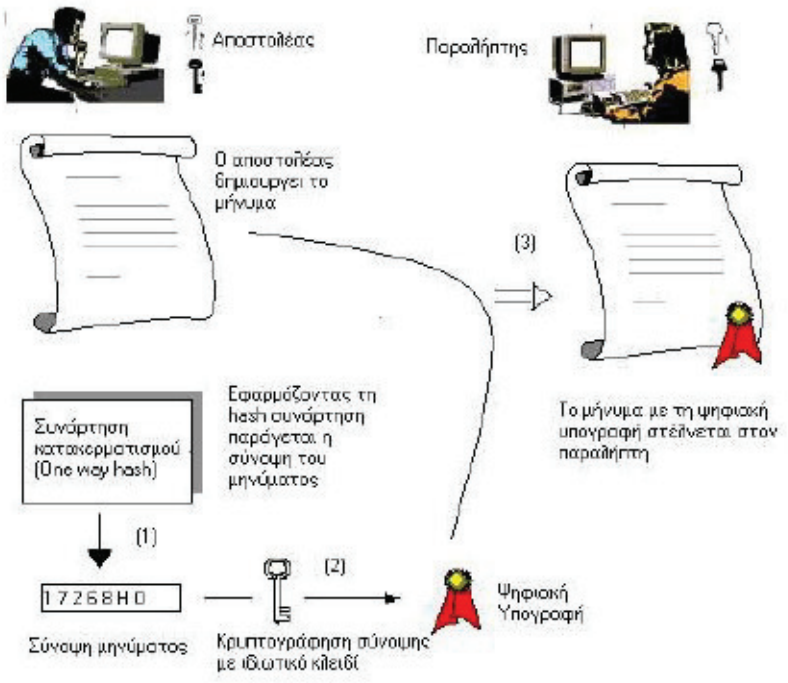
ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Η ανάπτυξη του Διαδικτύου, το ηλεκτρονικό εμπόριο και οι συναλλαγές μέσω ανοιχτών δικτύων καθιστούν επιτακτική την ανάγκη ασφάλειας, η οποία εξαρτάται σε μεγάλο βαθμό από την υπογραφή, την ταυτότητα δηλαδή των συναλλασσομένων. Ο χρήστης που συναλλάσσεται ηλεκτρονικά απαιτεί τα δεδομένα (μήνυμα ή κείμενο) που στέλνει να μην μπορούν να αποκαλυφθούν ή να διατεθούν σε μη εξουσιοδοτημένα άτομα (εμπιστευτικότητα). Τα δεδομένα απαγορεύεται να αλλοιωθούν κατά τη μετάδοσή τους. Ο παραλήπτης θα πρέπει να λάβει τα δεδομένα που του στάλθηκαν, χωρίς αυτά να έχουν τροποποιηθεί στο ελάχιστο (ακεραιότητα). Σε μια τέτοια συναλλαγή, ο παραλήπτης πρέπει να είναι βέβαιος για την ταυτότητα του αποστολέα (αυθεντικότητα). Η συμμετοχή σε μία ηλεκτρονική συναλλαγή προϋποθέτει ότι τα εμπλεκόμενα μέρη δεν έχουν νόμιμο δικαίωμα να αρνηθούν εκ των υστέρων τη συμμετοχή τους στη συναλλαγή αυτή (μη αποποίηση ευθύνης).

7.1 Η Έννοια της ψηφιακής υπογραφής.

Με τον όρο ηλεκτρονική υπογραφή δεν εννοούμε την αποτύπωση της ιδιόχειρης υπογραφής ούτε την μεταβίβασή της με ηλεκτρονικά μέσα, αλλά ένα ευρύτερο σύνολο μεθόδων υπογραφής για τον προσδιορισμό του συντάκτη του ηλεκτρονικού μηνύματος. Είναι μία μέθοδος τεκμηρίωσης με ηλεκτρονικά μέσα, που χρησιμοποιείται σε συγκεκριμένες μηχανικές απεικονίσεις (εγγραφές δεδομένων σε μαγνητικά μέσα ηλεκτρονικού υπολογιστή, συμπεριλαμβανομένης της ηλεκτρονικής ανταλλαγής δεδομένων και της ηλεκτρονικής αλληλογραφίας), με σκοπό την διασφάλιση αφενός της γνησιότητας και της ακρίβειας του περιεχομένου του ηλεκτρονικού εγγράφου και αφετέρου της εξατομίκευσης του εκδότη του εγγράφου αυτού.Για την δημιουργία και τις εφαρμογές της ηλεκτρονικής υπογραφής είναι δυνατόν να χρησιμοποιούνται σύγχρονες τεχνολογίες είτε υλικού (hardware) είτε λογισμικού (software) ηλεκτρονικών υπολογιστών, που επιλέγονται συνήθως από το πρόσωπο που επιδιώκει να αποκτήσει ηλεκτρονική υπογραφή, ώστε να προσδιορίζεται αξιόπιστα η ταυτότητά του στις ηλεκτρονικές συναλλαγές. Η ιδιόχειρη υπογραφή, που δεν είναι τεχνικά δυνατή στα ηλεκτρονικά έγγραφα, διότι λείπει η υλική ενσωμάτωση, υποκαθίσταται στην ηλεκτρονική επικοινωνία από την ηλεκτρονική υπογραφή. Υπάρχουν πολλοί τρόποι ηλεκτρονικής υπογραφής από την ατελέστερη μορφή των κωδικών (password) και των μυστικών κωδικών αριθμών (PIN) μέχρι τις πιο σύνθετες περιπτώσεις με χρήση κρυπτογραφικών ή βιομετρικών μεθόδων. Στην έννοια της ηλεκτρονικής υπογραφής περιλαμβάνεται και η ψηφιακή υπογραφή, η οποία δεν αποτελεί τίποτε περισσότερο από μία ασφαλή μέθοδο διαπίστωσης τόσο του εκδότη ηλεκτρονικού κειμένου, όσο και της γνησιότητας και του αναλλοίωτου αυτού. Η ψηφιακή υπογραφή, όπως είδαμε, είναι μία μέθοδος

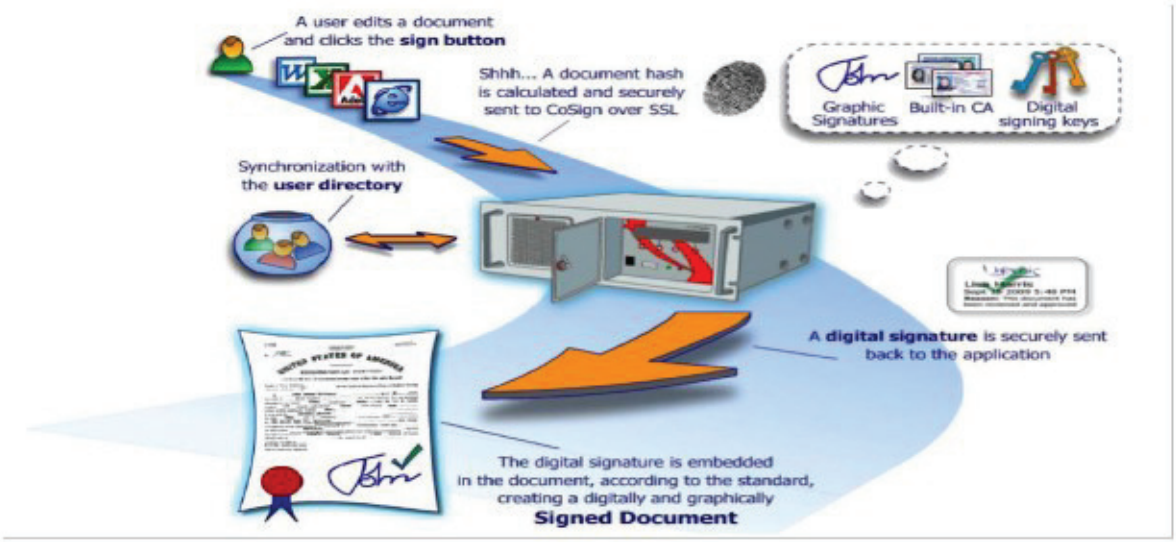
κρυπτογράφησης ενός κειμένου,που εγγυάται την αυθεντικότητα και την μη αλλοίωση του κειμένου αυτού. Τα συστήματα παραγωγής ψηφιακής υπογραφής διαθέτουν τους κατάλληλους μηχανισμούς, ώστε να διασφαλίζεται ότι ένα έγγραφο είναι γνήσιο, ότι δημιουργήθηκε από τον υπογράφοντα και ενδεχομένως ότι ο χρόνος σύνταξης του εγγράφου είναι ο αναφερόμενος.



Τα κρυπτογραφικά συστήματα αποτελούνται από κρυπτογραφικούς αλγόριθμους, δηλαδή από ένα σύνολο μαθηματικών συναρτήσεων, που χρησιμοποιούνται στην κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Τα κυριότερα συστήματα κρυπτογράφησης είναι δύο: το συμμετρικό και το ασύμμετρο σύστημα κρυπτογράφησης. Το σύστημα που χρησιμοποιεί συμμετρικούς αλγόριθμους, όπως είναι το DES (Data Encryption Standard), διαθέτει το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση, το οποίο είναι γνωστό τόσο στον αποστολέα όσο και στον παραλήπτη. Γι' αυτό το εν λόγω σύστημα είναι πρόσφορο για κλειστή ομάδα συναλλασσομένων και όχι για συναλλακτική επαφή με μεγάλο αριθμό συναλλασσομένων. λλασσομένων και όχι για συναλλακτική επαφή με μεγάλο αριθμό συναλλασσομένων.
Το δεύτερο κρυπτογραφικό σύστημα, αυτό της ασύμμετρης κρυπτογράφησης, χρησιμοποιεί ασύμμετρους αλγόριθμους (ασύμμετρη μέθοδος κρυπτογράφησης RSA). Για την θέση της ψηφιακής υπογραφής εφαρμόζεται ένας συνδυασμός δημοσίου και μυστικού κλειδιού. Με την βοήθεια ενός ειδικού προγράμματος παράγεται καταρχάς μία σύντμηση του μεταβιβαζόμενου κειμένου, ένα είδος περίληψής του. Το συντμημένο αυτό κείμενο σφραγίζεται με το μυστικό κλειδί.
Το μυστικό ιδιωτικό κλειδί είναι γνωστό μόνο στον αποστολέα του μηνύματος, ο οποίος το χρησιμοποιεί για την κρυπτογράφηση του μηνύματος. Το κλειδί αυτό αποθηκεύεται στον σκληρό δίσκο του υπολογιστή ή σε ειδική κάρτα ηλεκτρονικού

υπολογιστή και ασφαλίζεται από τρίτους. Στην πράξη ασφαλίζεται συνήθως η κάρτα ηλεκτρονικού υπολογιστή με έναν αριθμό PIN. Ο συνδυασμός του μηνύματος με το μυστικό κλειδί αποτελεί την ψηφιακή υπογραφή του αποστολέα. Κατόπιν μεταδίδεται το κρυπτογραφημένο κείμενο στον παραλήπτη, ο οποίος το αποκρυπτογραφεί με την χρήση του δημοσίου κλειδιού του συντάκτη, το οποίο είτε αποστέλλεται στον παραλήπτη μαζί με το κρυπτογραφημένο κείμενο είτε ξεχωριστά είτε δημοσιεύεται σε έναν δημόσιο on line κατάλογο.Έτσι, ένα πρόγραμμα ελέγχου του παραλήπτη ξεκλειδώνει με το δημόσιο κλειδί το συντμημένο κείμενο και παράγει συγχρόνως μία δεύτερη σύντμηση του παραληφθέντος ηλεκτρονικού κειμένου. Αν τα δύο συντμημένα κείμενα είναι όμοια, πιστοποιείται η προέλευση του κειμένου από τον υπογράφοντα. Η ασύμμετρη κρυπτογραφική μέθοδος είναι προσφορότερη για τα ανοικτά δίκτυα, όπως το Ίντερνετ, ωστόσο δεν είναι κατάλληλη για μεταβίβαση εκτενών μηνυμάτων, επειδή είναι χρονοβόρα. Για τον λόγο αυτό για την αποστολή εκτενών μηνυμάτων ακολουθείται μία διαφορετική διαδικασία, κατά την οποία δημιουργείται πρώτα το «δακτυλικό αποτύπωμα» του κειμένου, εξάγεται δηλαδή το άθροισμα των bits, εκ των οποίων συγκροτείται το περιεχόμενο του κειμένου. Αυτό το «δακτυλικό αποτύπωμα» υπογράφεται στην συνέχεια, κρυπτογραφείται δηλαδή με την διαδικασία RSA. Ο αποστολέας κρυπτογραφεί έτσι την περίληψη του κειμένου αυτού μαζί με άλλα πρόσθετα δεδομένα, όπως ο τόπος και ο χρόνος της υπογραφής, με την χρήση του μυστικού κλειδιού. Ο παραλήπτης με την χρήση του δημόσιου κλειδιού αποκρυπτογραφεί το «δακτυλικό αποτύπωμα», ώστε να διαπιστώσει αν το περιεχόμενό του παρέμεινε αναλλοίωτο.

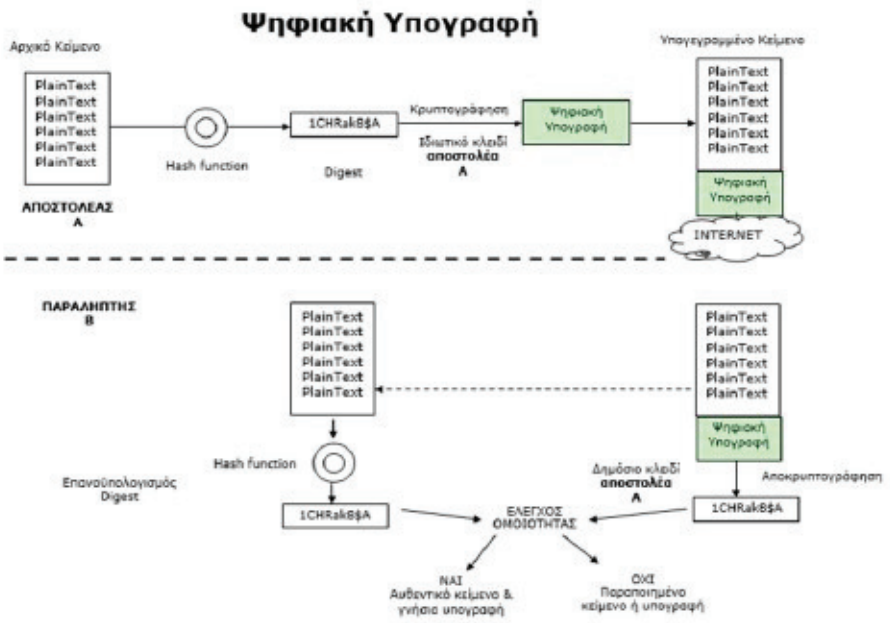
Άξιο αναφοράς είναι και το σύστημα του «ψηφιακού φακέλου», που αποτελεί συνδυασμό του συμμετρικού και του ασύμμετρου κρυπτογραφικού συστήματος. Κατά το σύστημα αυτό κρυπτογραφείται το κείμενο από τον αποστολέα με έναν συμμετρικό αλγόριθμο και με την χρήση ενός σύντομου ασφαλούςκλειδιού, που καταστρέφεται μετά την ολοκλήρωση της επικοινωνίας και ονομάζεται γι’ αυτό κλειδί συνεδρίας. Το κλειδί αυτό για ασφάλεια κρυπτογραφείται με έναν ασύμμετρο αλγόριθμο. Ο παραλήπτης του κειμένου πρέπει πρώτα να αποκρυπτογραφήσει το κλειδί συνεδρίας με το δημόσιο κλειδί και στην συνέχεια και το μήνυμα



7.2 Η ψηφιακή υπογραφή ως υποκατάστατο της ιδιόχειρης υπογραφής στις ηλεκτρονικές συναλλαγές.

Για να θεωρηθεί η ψηφιακή υπογραφή ως υποκατάστατο της ιδιόχειρης, πρέπει να εξετασθεί αν αυτή πληρεί τις βασικές λειτουργίες της ιδιόχειρης υπογραφής, δηλαδή την αποδεικτική λειτουργία, την λειτουργία προσδιορισμού της ταυτότητας του εκδότη και την λειτουργία επιβεβαίωσης της ταυτότητας του εγγράφου. Η ψηφιακή υπογραφή δύναται να αναπληρώσει την ιδιόχειρη υπογραφή στις ηλεκτρονικές συναλλαγές, καθώς πληρεί τις βασικές λειτουργίες που πληρεί και η τελευταία, δηλαδή:
α) την αποδεικτική λειτουργία, στο μέτρο που συμπεραίνεται ότι το έγγραφο προέρχεται από τον υπογράφοντα με την βοήθεια του πιστοποιητικού που παρέχεται από τους παρόχους υπηρεσιών πιστοποίησης. Λειτουργίες πιστοποίησης επιτελούν οι πάροχοι υπηρεσιών πιστοποίησης, οι οποίες υπηρεσίες συνίστανται στην επιβεβαίωση της αυθεντικότητας του ιδιοκτήτη και των χαρακτηριστικών ενός δημόσιου κλειδιού με την έκδοση ενός πιστοποιητικού, μίας ηλεκτρονικής βεβαίωσης σχετικά με την ταυτότητα ενός ατόμου.Το παρεχόμενο πιστοποιητικό πρέπει να περιλαμβάνει ένδειξη ότι το πιστοποιητικό εκδίδεται ως αναγνωρισμένο πιστοποιητικό, τα στοιχεία αναγνώρισης του Παρόχου Υπηρεσιών Πιστοποίησης και το κράτος στο οποίο είναι εγκατεστημένος, το όνομα του υπογράφοντος ή ψευδώνυμο που αναγνωρίζεται ως ψευδώνυμο, πρόβλεψη ειδικού χαρακτηριστικού του υπογράφοντος, που θα περιληφθεί, εφόσονείναι σημαντικό σε σχέση με τον σκοπό για τον οποίο προορίζεται το πιστοποιητικό, δεδομένα επαλήθευσης υπογραφής που αντιστοιχούν σε δεδομένα δημιουργίας υπογραφής υπό τον έλεγχο του υπογράφοντος, ένδειξη της έναρξης και του τέλους της περιόδου ισχύος του πιστοποιητικού, τον κωδικό ταυτοποίησης του πιστοποιητικού, την προηγμένη ηλεκτρονική υπογραφή τουΠαρόχου Υπηρεσιών Πιστοποίησης που το εκδίδει, τυχόν περιορισμούς του πεδίου χρήσης του πιστοποιητικού και τυχόν όρια στο ύψος των συναλλαγών, για τις οποίες το πιστοποιητικό μπορεί να χρησιμοποιηθεί.

β) την λειτουργία προσδιορισμού της ταυτότητας του εκδότη, καθόσον τα κλειδιά της ψηφιακής υπογραφής παρέχονται από τους Παρόχους Υπηρεσιών Πιστοποίησης σε συγκεκριμένα πρόσωπα, με τα οποία συνδέονται συμβατικά
γ) την λειτουργία επιβεβαίωσης της ταυτότητας του εγγράφου, καθώς με την διαδικασία επαλήθευσης της ψηφιακής υπογραφής είναι δυνατή η διαπίστωση της αλλοίωσης ή όχι του περιεχομένου του ηλεκτρονικού εγγράφου, και
δ) την εγγυητική λειτουργία, επειδή ο αποστολέας ενός ηλεκτρονικού εγγράφου με την ψηφιακή του υπογραφή αναλαμβάνει την ευθύνη για την γνησιότητα και την ακρίβεια του περιεχομένου του εγγράφου.



7.3 Νομικά ζητήματα.

Η ανοδική τάση που παρατηρείται στη χρήση ηλεκτρονικών μέσων επικοινωνίας τα τελευταία χρόνια οφείλεται στα τεράστια πλεονεκτήματα που προσφέρουν. Εντούτοις, τα πλεονεκτήματα αυτά τότε μόνο μπορούν να αξιοποιηθούν πλήρως, όταν αφενός υπάρχει ευρύτερη νομική αναγνώριση της ηλεκτρονικής επικοινωνίας και αφετέρου η γνησιότητα των μηνυμάτων είναι εξασφαλισμένη. Οι δύο αυτές προϋποθέσεις, η μία νομική και η άλλη τεχνική, είναιαπαραίτητες για την εδραίωση του ηλεκτρονικού εμπορίου. Αρκετά ζητήματα που ανακύπτουν από τη χρησιμοποίηση των νέων μέσων μπορούν, με κατάλληλη ερμηνεία των παραδοσιακών κανόνων δικαίου που βασίζονται στον έγγραφο τύπο, να επιλυθούν χωρίς νομοθετική παρέμβαση. Ουσιαστικές δυσκολίες μπορούν να υπάρξουν από πλευράς φορολογικού δικαίου, η γραφειοκρατική παρέμβαση του οποίου στις συναλλαγές είναι εντονότατη. Το ίδιο ισχύει και με την επιβολή χαρτοσήμανσης.
Γενικότερα η νέα τεχνολογία δεν μεταβάλλει στο συναλλακτικό πεδίο την ουσία των κανόνων του εμπορικού δικαίου. Απλώς καταργεί σε μεγάλο βαθμό τις προσωπικές σχέσεις μεταξύ των συναλλασσομένων και εισάγει και στο εμπορικό δίκαιο το απρόσωπο στοιχείο, ίδιο των καιρών μας, αλλά και τη "βιομηχανοποίηση" της

πληροφόρησης και της επικοινωνίας. Η συνεχώς αυξανόμενη χρήση του Διαδικτύου για τη σύναψη εμπορικών συμβάσεων, τοηλεκτρονικό εμπόριο, και οι ανυπολόγιστες επιδράσεις του στην οικονομία, δραστηριοποίησαν διεθνείς οργανισμούς, την Επιτροπή Ευρωπαϊκών Κοινοτήτων καθώς και κυβερνήσεις διαφόρων χωρών, προκειμένου να ορίσουν το νομικό πλαίσιο των ηλεκτρονικών συναλλαγών
Σε διεθνές επίπεδο, η Επιτροπή Διεθνούς Εμπορικού Δικαίου των Ηνωμένων Εθνών (UNCITRAL) συνέταξε το 1996 τον Πρότυπο Νόμο για το ηλεκτρονικό εμπόριο, ρυθμίζοντας ζητήματα όπως η εξομοίωση των ηλεκτρονικών πληροφοριών με έγγραφα υλικής υπόστασης, η νομική ισχύς της ηλεκτρονικής υπογραφής, η αποδεικτική δύναμη των ηλεκτρονικών κειμένων, ο τόπος, χρόνος και απόδειξη παραλαβής του ηλεκτρονικού μηνύματος.
, χρόνος και απόδειξη παραλαβής του ηλεκτρονικού μηνύματος. Η Ευρωπαϊκή Ένωση, αναγνωρίζοντας την ανάγκη νομικής ρύθμισης των ηλεκτρονικών εμπορικών συναλλαγών, εξέδωσε Οδηγία για το ηλεκτρονικό εμπόριο. Συγκεκριμένα, το Ευρωπαϊκό Κοινοβούλιο προέβη το 1999 στην έκδοση της υπ' αριθμ. 2000/31/ΕΚ Οδηγίας, η οποία τέθηκε σε ισχύ στις 17/07/2000. Με την Οδηγία αυτή καθιερώθηκε η αρχή της ελευθερίας σύναψης ηλεκτρονικών συμβάσεων, η αρχή της χώρας προέλευσης, που σήμαινε ότι το Δίκαιο που διέπει τις συναλλαγές με ηλεκτρονικά μέσα είναι το Δίκαιο της χώρας μόνιμης εγκατάστασης του φορέα παροχής υπηρεσιών, και ο εξωδικαστικός διακανονισμός των διαφορών που θα προκύψουν ψουν. Το Ευρωκοινοβούλιο, προκειμένου να διασφαλίσει τη γνησιότητα της ηλεκτρονικής υπογραφής, προέβλεψε την έκδοση αναγνωρισμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής, μιας ηλεκτρονικής βεβαίωσης, η οποία συνδέει δεδομένα επαλήθευσης της υπογραφής με ένα φυσικό πρόσωπο, επιβεβαιώνοντας έτσι την ταυτότητά του.
Η Ελλάδα, με την έκδοση του υπ' αριθμ. 150/2001 Π.Δ. εναρμονίστηκε με την Οδηγία αυτή και προέβη σε σημαντικά βήματα προς τη θέσπιση ενός "Δικαίου του Internet". Χαρακτηριστικό παράδειγμα αποτελεί ο Ν. 2672/1999 για τις ηλεκτρονικές υπογραφές καθώς και ο Ν. 2251/1994 για την προστασία των καταναλωτών.
Η νομοθετική ρύθμιση για τις ηλεκτρονικές υπογραφές αποτελεί το πρώτο βήμα για την καθιέρωση στην χώρα μας ενός νομικού πλαισίου, που θα προάγει το ηλεκτρονικό εμπόριο. Περιλαμβάνει διατάξεις, που αναφέρονται σε μεγάλο βαθμό σε τεχνικές απαιτήσεις και προϋποθέσεις, ώστε να αξιοποιηθεί κατά τον ασφαλέστερο τρόπο η ηλεκτρονική υπογραφή στην συναλλακτική ζωή.Με την χρήση μίας ιδιαίτερα πρωτοποριακής αλλά και περίπλοκης ορολογίας καταλαμβάνονται από τους ορισμούς του π. δ. 150/2001 όλες οι γνωστές ως σήμερα μορφές υπογραφής με ηλεκτρονικά μέσα, ενώ ταυτόχρονα η ευρέως διατυπωθείσα ορολογία διέπεται από τεχνολογική ουδετερότητα, ώστε να μπορούν να ενταχθούν στο πεδίο της τυχόν νέες μορφές ηλεκτρονικής υπογραφής με αντίστοιχα χαρακτηριστικά. Η προσθήκη ωστόσο διαζευκτικά δίπλα στην έννοια της προηγμένης ηλεκτρονικής υπογραφής ως συνώνυμής της την ψηφιακή υπογραφή στο άρθρο 2 περ. 2 του π. δ. 150/2001 φαίνεται ότι δεν λαμβάνει υπόψη την περίπτωση μελλοντικών τεχνικών εφαρμογών αναγνώρισης της γνησιότητας ηλεκτρονικών εγγράφων, που θα πληρούν τις προϋποθέσεις της προηγμένης ηλεκτρονικής υπογραφής, χωρίς ωστόσο να βασίζονται

στην ασύμμετρη κρυπτογράφηση. Τυχόν καινούριες μέθοδοι κρυπτογράφησης, οι οποίες θα ανταποκρίνονται στις αόριστα διατυπωμένες προϋποθέσεις της προηγμένης ηλεκτρονικής υπογραφής (α: μονοσήμαντη σύνδεση με τον υπογράφοντα, β: ικανότητα ταυτοποίησης του υπογράφοντα, γ: δημιουργία της με μέσα, τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο, και δ: σύνδεσης με τα δεδομένα, στα οποία αναφέρεται, κατά τρόπο, ώστε να μπορεί να εντοπισθεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων), θαώστε να μπορεί να εντοπισθεί οποιαδήποτε επακόλουθη αλλοίωση των εν λόγω δεδομένων), θα τίθεται εν αμφιβόλω λόγω της εξίσωσης αυτής της προηγμένης ηλεκτρονικής υπογραφής με την ψηφιακή και τη δυνατότητα που θα υπάρχει για να ενταχθούν στην ευρέως διατυπωμένη έννοια της προηγμένης ηλεκτρονικής υπογραφής
Ένα επιπρόσθετο ζήτημα που τίθεται είναι το κατά πόσο είναι πρακτικά εφικτή η συντήρηση ως αποδεικτικών μέσων των στοιχείων της ηλεκτρονικά συναπτόμενης συναλλαγής.. Αυτό απαιτεί την αποθήκευση των ηλεκτρονικών δεδομένων σε συνθήκες, που εγγυώνται την αναλλοίωτη διατήρησή τους για μεγάλο χρονικό διάστημα, τουλάχιστον μέχρι την παρέλευση του χρόνου παραγραφής των σχετικών αξιώσεων.Στον ίδιο βαθμό απαιτείται η διατήρηση συμβατών τεχνολογικών μέσων, που χρησιμοποιούνται για την αναπαράσταση των δεδομένων αυτών και στο μέλλον, αν και η τεχνολογική πρόοδος καθιστά ταχεία την απαξίωση και την αντικατάστασή τους από νεότερα ,και αρκετές φορές μη συμβατά, μέσα.

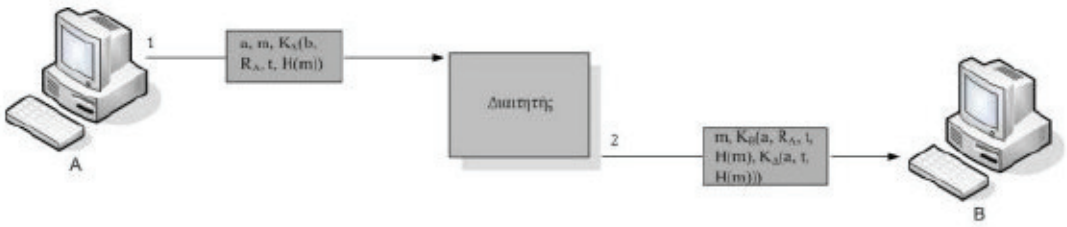
Η πρόβλεψη τρίτου έμπιστου προσώπου –του παρόχου υπηρεσιών πιστοποίησης- με πολύ σημαντικό ρόλο στην πιστοποίηση της ηλεκτρονικά καταρτιζόμενης συναλλαγής, στην εμπέδωσητης ασφάλειας στον χώρο του ηλεκτρονικού εμπορίου και στην διατήρηση αποδεικτικών στοιχείων αποτελεί σημαντικότατο παράγοντα –από κοινού με τις έννομες συνέπειες που αποδίδονται κυρίως στην προηγμένη, αλλά και στην απλή ηλεκτρονική υπογραφή- για τηνεπίτευξη του σκοπού της ενίσχυσης της εμπιστοσύνης των συναλλασσομένων προς το ηλεκτρονικό εμπόριο. Απεκδύεται έτσι η λειτουργία της υπογραφής, το αποκλειστικό προσωπικό στοιχείο, που την διακρίνει στην παραδοσιακή της μορφή, και συνδυάζεται απαραίτητα με έναολοκληρωμένο σύστημα υπηρεσιών πληροφορικής, που δεν ελέγχεται απολύτως από τον υπογράφοντα, αλλά βασίζεται στην αξιοπιστία και στην προηγμένη τεχνολογική υποδομή των παρόχων υπηρεσιών πιστοποίησης.
Για την απόδειξη της γνησιότητας ενός εγγράφου, χρησιμοποιούνται οι συμβατικές υπογραφές. Ειδικότερα, η υπογραφή αποτελεί μαρτυρία της εγκυρότητας του υπογεγραμμένου εγγράφου έτσι ώστε ο υπογράφων να μη μπορεί να το απαρνηθεί. Στις συναλλαγές ηλεκτρονικούεμπορίου καθίσταται αναγκαία η χρησιμοποίηση ενός ηλεκτρονικού ισοδύναμου της συμβατικής υπογραφής, δηλαδή μιας ηλεκτρονικής υπογραφής. Ο μηχανισμός της ηλεκτρονικής υπογραφής θα πρέπει να παρέχει απόδειξη της προέλευσης, της γνησιότητας και της ακεραιότητας των ανταλλασσόμενων μηνυμάτων. Απαιτείται δηλαδή ένα σύστημα μέσω του οποίου κάποιος θα μπορεί να στείλει ένα υπογεγραμμένο μήνυμα σε κάποιον άλλο με τέτοιο τρόπο ώστε:
⊣ Ο παραλήπτης να μπορεί να επιβεβαιώνει την ταυτότητα που δηλώνει ο

αποστολέας.
- Ο αποστολέας να μη μπορεί αργότερα να αρνηθεί το περιεχόμενο του μηνύματος.
- Ο παραλήπτης να μη μπορεί να κατασκευάσει το μήνυμα από μόνος του.

Οι ηλεκτρονικές υπογραφές που βασίζονται στην κρυπτογραφία ονομάζονται ψηφιακές υπογραφές. Η ψηφιακή υπογραφή εξαρτάται άμεσα από το μήνυμα το οποίο στέλνεται, είναι γνωστή μόνο στον αποστολέα αλλά μπορεί να επιβεβαιωθεί από τον καθένα. Η ψηφιακή υπογραφή θα πρέπει να είναι εύκολο να υπολογιστεί και να επιβεβαιωθεί από οποιονδήποτε ενδιαφερόμενο. Παράλληλα όμως θα πρέπει να είναι αδύνατο να αντιγραφεί.
Η ψηφιακή υπογραφή είναι άμεσα συσχετιζόμενη με το μήνυμα το οποίο στέλνεται και δεν είναι ποτέ η ίδια. Διαφορετικό μήνυμα σημαίνει άμεσα και διαφορετική ψηφιακή υπογραφή. Η «σύνδεση» της ψηφιακής υπογραφής με το περιεχόμενο του μηνύματος που υπογράφει εξασφαλίζει την ακεραιότητα των δεδομένων (data integrity). Δηλαδή διασφαλίζει ότι από τη στιγμή που ο αποστολέας υπέγραψε τα δεδομένα, αυτά δεν έχουν τροποποιηθεί.

7.4 Υπογραφές με Κρυπτογραφία Μυστικού Κλειδιού.

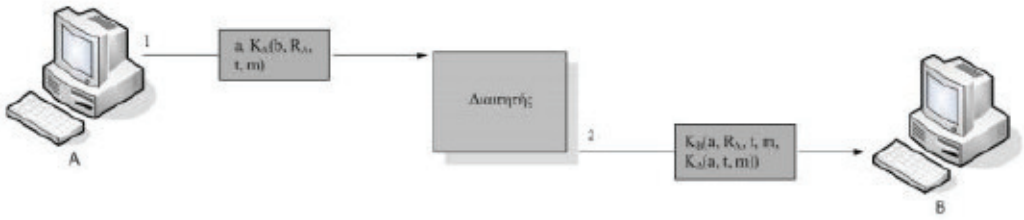
Στις υπογραφές με κρυπτογραφία μυστικού κλειδιού χρησιμοποιείται μια κεντρική εξουσία, η οποία υπογράφει και επιβεβαιώνει την ψηφιακή υπογραφή. Την εξουσία αυτή την ονομάζουμε «διαιτητή», διότι χρησιμοποιείται για να επιλύει διαφορές που μπορεί να προκύψουν. Ο διαιτητής γνωρίζει τα πάντα και τον εμπιστεύονται οι πάντες. Τονίζεται ότι η λειτουργία του όλου σχήματος βασίζεται στην εμπιστοσύνη που έχουν προς τον διαιτητή τα δύο μέρη που θέλουν να επικοινωνήσουν.
Υποθέτουμε πως ο χρήστης Α θέλει να επικοινωνήσει με τον χρήστη Β. Ο χρήστης Β με τη σειρά του θέλει κάποια μορφή εξασφάλισης σχετικά με την αυθεντικοποίηση της ταυτότητας του Α. Επίσης χρειάζεται να γνωρίζει, με κάποιο τρόπο, πως τα περιεχόμενα όλων των μηνυμάτων δεν έχουν μεταβληθεί (ακούσια ή εκούσια). Τέλος ο χρήστης Β θέλει ένα τρόπο εξασφάλισης των μηνυμάτων του χρήστη Α ώστε να μην μπορεί κάποια στιγμή εκείνος να αρνηθεί το γεγονός ότι έχει στείλει τα συγκεκριμένα μηνύματα
Κάθε χρήστης μοιράζεται ένα συμμετρικό κλειδί με τον διαιτητή. Το κλειδί αυτό το γνωρίζει μόνο ο συγκεκριμένος χρήστης και ο διαιτητής. Όταν ο χρήστης Α θέλει να στείλει ένα υπογεγραμμένο μήνυμα στο χρήστη Β, και δεν απαιτείται μυστικότητα, δηλαδή δεν ενδιαφέρει τον χρήστη Α αν το συγκεκριμένο μήνυμα διαβαστεί από κάποιον τρίτο, τότε εκτελείται η ακολουθία μηνυμάτων που απεικονίζεται στο Σχήμα7-1



Σχήμα 7-1: Ψηφιακές Υπογραφές χωρίς μυστικότητα.

Ο χρήστης Α υπολογίζει με χρήση ειδικού λογισμικού τη σύνοψη του μηνύματος m που θέλει να στείλει στον χρήστη Β, Η(m). Στη συνέχεια δημιουργεί το ΚΑ(b, RA, t, Η(m)), όπου με b παριστάνεται η ταυτότητα του Β, RA είναι η πρόκληση από τον χρήστη Α και t μια χρονοσφραγίδα. Δηλαδή κρυπτογραφεί τη σύνοψη του μηνύματος Η(m), και τα b, RA, t, με το μυστικό κλειδί που μοιράζεται με τον διαιτητή. Έπειτα στέλνει στον διαιτητή την ταυτότητα του, a, το μήνυμα m σε καθαρή μορφή και το ΚΑ(b, RA, t, Η(m)).
Όταν ο διαιτητής λάβει το μήνυμα 1, βλέπει ότι είναι από τον Α. Αποκρυπτογραφεί το μήνυμα 1 και στέλνει στον Β το μήνυμα 2. Το μήνυμα 2 περιέχει το μήνυμα m σε καθαρή μορφή και τα a, RA, t, Η(m), ΚΔ (a, t, Η(m)) κρυπτογραφημένα με το κλειδί ΚΒ που μοιράζεται ο διαιτητής με τον Β. ΚΔ είναι το κλειδί του διαιτητή. Ο Β μόλις λάβει το μήνυμα 2 υπολογίζει ι την σύνοψη μηνύματος εφαρμόζοντας στο μήνυμα m την ίδια συνάρτηση κατακερματισμού με τον αποστολέα, ελέγχοντας αν αυτή είναι ίδια με την σύνοψη μηνύματος που περιέχεται κρυπτογραφημένη στο μήνυμα 2. Αν οι δύο συνόψεις ταυτίζονται, τότε το μήνυμα δεν τροποποιήθηκε από τη στιγμή που υπογράφηκε από τον διαιτητή
Ο χρήστης Α δεν μπορεί να αργότερα να αρνηθεί ότι έστειλε το συγκεκριμένο μήνυμα διότι ο Β έχει αποδείξεις: Είναι γνωστό ότι ο διαιτητής δεν μπορεί να δεχθεί ένα μήνυμα από τονΑ παρά μόνο αν αυτό είναι κρυπτογραφημένο με ΚΑ. Επιπλέον ο διαιτητής μόλις λάβει το μήνυμα 1 υπολογίζει την σύνοψη μηνύματος του m και ελέγχει αν αυτή είναι ίδια με την σύνοψη μηνύματος που περιέχεται κρυπτογραφημένη στο μήνυμα 1. Εφόσον το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί μετά την αποστολή του, οι συνόψεις ταυτίζονται. Έτσι ο διαιτητής βεβαιώνει την αυθεντικότητα του μηνύματος και δεν υπάρχει πιθανότητα ένας εισβολέας να έστειλε στον διαιτητή ένα μήνυμα εκ μέρους του Α. Ο Β έχει ως αποδεικτικό στοιχείο για την ταυτότητα του Α το υπογεγραμμένο μήνυμα ΚΔ (a, t, Η(m)), το οποίο προέρχεταιαπό τον διαιτητή. Όταν ο διαιτητής, τον οποίο εμπιστεύονται όλοι, αποκρυπτογραφήσει το μήνυμα αυτό αποδεικνύετε ότι ο Α έστειλε κάποιο μήνυμα που έχει σύνοψη Η(m) στον Β. Επιπλέον δεν μπορεί αργότερα ο Α να ισχυριστεί ότι έστειλε στον Β κάποιο άλλο μήνυμα με την ίδια σύνοψη Η(m), διότι πρακτικά δεν υπάρχουν δύο διαφορετικά μηνύματα που να έχουν την ίδια σύνοψη μηνύματος
Το πρωτόκολλο που περιγράφεται στο Σχήμα 7-1 χρησιμοποιεί χρονοσφραγίδες για να αποτρέψει τυχόν επιθέσεις επανάληψης. Επιπλέον ο χρήστης Β μπορεί να ελέγχει

όλα τα πρόσφατα μηνύματα ώστε να βλέπει αν το RA χρησιμοποιήθηκε σε κάποιο από αυτά. Αν συμβαίνει κάτι τέτοιο το μήνυμα απορρίπτεται ως επανάληψη.
Όταν ο χρήστης Α θέλει να στείλει ένα υπογεγραμμένο μήνυμα στο χρήστη Β, και απαιτείται μυστικότητα, δηλαδή ο χρήστης Α δε θέλει κανένας άλλος, εκτός από τον Β και τον διαιτητή, να διαβάσει το συγκεκριμένο μήνυμα, τότε εκτελείται η ακολουθία μηνυμάτων που απεικονίζεται στο Σχήμα 7-2.

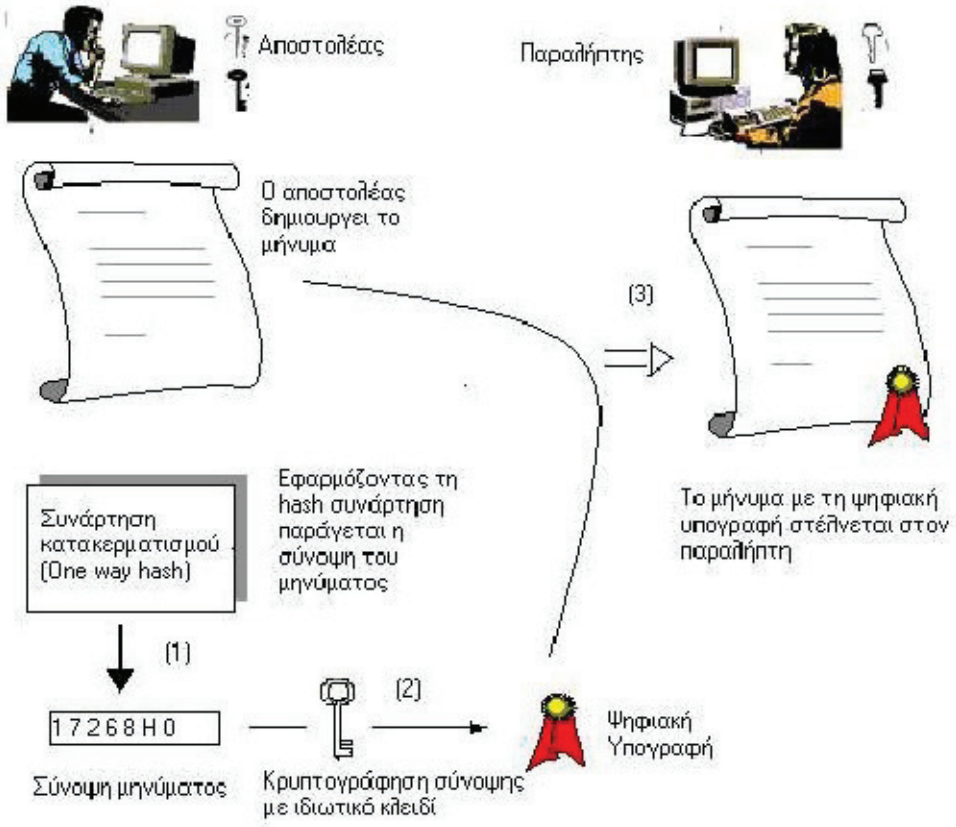


Σχήμα 7-2: Ψηφιακές Υπογραφές με μυστικότητα.

Ο χρήστης Α δημιουργεί το ΚΑ(b, RA, t, m), όπου m είναι το μήνυμα που θέλει να στείλει στον Β, και το στέλνει στον διαιτητή μαζί με την ταυτότητα του, a. Όταν ο διαιτητής λάβει το μήνυμα 1, βλέπει ότι είναι από τον Α. Αποκρυπτογραφεί το μήνυμα 1 και στέλνει στον Β το μήνυμα 2. Το μήνυμα 2 περιέχει τα a, RA, t, m, ΚΔ (a, t, m) κρυπτογραφημένα με το κλειδί ΚΒ που μοιράζεται ο διαιτητής με τον Β.
Ο Β στη συνέχεια αποκρίνεται στην απαίτηση του Α. Και σε αυτό το πρωτόκολλο ο χρήστης Α δεν μπορεί να αργότερα να αρνηθεί ότι έστειλε το συγκεκριμένο μήνυμα διότι ο Β έχει τις ίδιες αποδείξεις με πριν.
Τα πρωτόκολλα ψηφιακής υπογραφής που απεικονίζονται στο Σχήμα 7-1 και στο Σχήμα 7-2 έχουν ουσιαστικά μόνο μια διαφορά: Στο πρωτόκολλο στο Σχήμα 7-1 κρυπτογραφείται η σύνοψη του μηνύματος m, ενώ στο πρωτόκολλο στο Σχήμα 7-2 κρυπτογραφείται το ίδιο το μήνυμα m. Το πρωτόκολλο που χρησιμοποιεί σύνοψη μηνύματος υπολογίζει πολύ πιο γρήγορα τις ψηφιακές υπογραφές σε σχέση με το πρωτόκολλο που χρησιμοποιεί κρυπτογραφία. Άρα εφόσον η κρυπτογραφία είναι μια αργή διαδικασία, στις περιπτώσεις που δεν απαιτείται μυστικότητα αλλά μόνο πιστοποίηση αυθεντικότητας, είναι προτιμότερο να χρησιμοποιείται το πρωτόκολλο που απεικονίζεται στο Σχήμα 7-1. Με τα πρωτόκολλα αυτά (Σχήμα 7-1 και Σχήμα 7-2) δύο χρήστες Α και Β μπορούν να επικοινωνούν μεταξύ τους χωρίς να χρειάζεται να μοιράζονται κάποιο κοινό κρυπτογραφικό κλειδί. Στις σημερινές εφαρμογές αυτό είναι αρκετά συνηθισμένο. Σε περίπτωση που δύο χρήστες θέλουν να επικοινωνήσουν, αλλά δεν υπάρχει αμοιβαία εμπιστοσύνη μεταξύ τους, το σχήμα αυτό μπορεί να δουλέψει αποτελεσματικά. Τα πρωτόκολλα αυτά μπορούν να χρησιμοποιηθούν και σε συναλλαγές ηλεκτρονικού εμπορίου, που λαμβάνουν χώρα στα πλαίσια ενός μεγάλου οργανισμού. Ο οργανισμός αυτός ελέγχει εταιρείες και χρήστες και τους δίνει την δυνατότητα να πραγματοποιούν ηλεκτρονικές συναλλαγές μεταξύ τους με βάση τα παραπάνω πρωτόκολλα. Στηνπερίπτωση αυτή ο χρήστης Α αντιπροσωπεύει τον αγοραστή, ο χρήστης Β τον πωλητή και ο ίδιος ο οργανισμός τον διαιτητή. Έτσι κάθε χρήστης-εταιρεία θα έχει ένα μυστικό κλειδί το οποίο θα γνωρίζει μόνο ο οργανισμός,

και με το κλειδί αυτό θα μπορεί να κάνει ηλεκτρονικές συναλλαγές στα πλαίσια όμως του συγκεκριμένου οργανισμού.

7.5 Υπογραφές με Κρυπτογραφία Δημοσίου Κλειδιού.



Ένα πρόβλημα που εμφανίζεται με τη χρήση κρυπτογραφίας μυστικού κλειδιού για τις ψηφιακές υπογραφές είναι ότι οι πάντες πρέπει να συμφωνήσουν ώστε να εμπιστεύονται μια συγκεκριμένη εξουσία, τον «διαιτητή». Επιπλέον ο διαιτητής είναι σε θέση να διαβάζει όλα τα υπογεγραμμένα μηνύματα. Θα ήταν επομένως καλύτερα αν τα υπογεγραμμένα έγγραφα δεν απαιτούσαν μια έμπιστη κεντρική εξουσία. Η κρυπτογραφία δημοσίου κλειδιού μπορεί να αποτελέσει σημαντική συνεισφορά για τη λύση αυτού του προβλήματος.
Η ασύμμετρη κρυπτογραφία παρέχει τη δυνατότητα πιστοποίησης της αυθεντικότητας ενός μηνύματος, με την παραγωγή μιας μοναδικής ψηφιακή υπογραφής. Η ψηφιακή υπογραφή αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί, ελέγχοντας την υπογραφή, να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι. Ο αποστολέας υπογράφει το μήνυμα με το ιδιωτικό τουκλειδί. Ο παραλήπτης διαθέτει το δημόσιο κλειδί του αποστολέα και μπορεί να επιβεβαιώσει ότι το μήνυμα υπογράφτηκε με το αντίστοιχο ιδιωτικό κλειδί. Εφόσον το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του, μόνο αυτός θα μπορούσε να το χρησιμοποιήσει, για

να υπογράψει κάποιο μήνυμα και επομένως μόνο αυτός θα μπορούσε να έχει στείλει το μήνυμα αυτό. Οπότε με την τεχνολογία της ασύμμετρης κρυπτογραφίας, διατηρώντας μυστικό το ένα κλειδί ως ιδιωτικό(δεδομένα δημιουργίας υπογραφής) και διανέμοντας ελεύθερα το άλλο κλειδί ως δημόσιο (δεδομένα επαλήθευσης υπογραφής), εξασφαλίζετε ότι όλοι όσοι γνωρίζουν ένα δημόσιο κλειδί μπορούν να επαληθεύσουν μια ψηφιακή υπογραφή που δημιουργείται από τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού. Συγκεκριμένα για να δημιουργηθεί μια ψηφιακή υπογραφή, απαιτούνται δύο βήματα:

- Ο αποστολέας υπολογίζει με χρήση ειδικού λογισμικού μια σύνοψη H(m) του μηνύματος m.
- Χρησιμοποιώντας το ιδιωτικό του κλειδί, ο αποστολέας κρυπτογραφεί τη σύνοψη που προέκυψε. Η ασύμμετρα κρυπτογραφημένη σύνοψη μαζί με την πληροφορία προσδιορισμού του αλγόριθμου σύνοψης, αποτελεί την ψηφιακή υπογραφή του μηνύματος. Στη συνέχεια ο αποστολέας αποστέλλει αυτή τη ψηφιακή υπογραφή μαζί με το αρχικό μήνυμα στον παραλήπτη.

Το ιδιωτικό κλειδί του αποστολέα δεν χρησιμοποιείται για την κρυπτογράφηση του ίδιου του κειμένου, αλλά μόνο για τη δημιουργία της ψηφιακής υπογραφής, δηλαδή την κρυπτογράφηση της σύνοψης, η οποία επισυνάπτεται στα δεδομένα που αποστέλλονται. Τα δεδομένα αυτά μπορεί να είναι είτε κρυπτογραφημένα, είτε μη κρυπτογραφημένα, ανάλογα με το επίπεδο μυστικότητας που είναι επιθυμητό. Ανεξαρτήτως πάντως της κρυπτογράφησης ή μη των δεδομένων, ο παραλήπτης μπορεί να συμπεράνει αν αυτά έχουν τροποποιηθεί και από πού αυτά προέρχονται, με τη βοήθεια του δημόσιου κλειδιού του αποστολέα. Συνολικά η επικύρωση της υπογραφής χρειάζεται τρία βήματα:

- Το δημόσιο κλειδί του αποστολέα χρησιμοποιείται από τον παραλήπτη για την αποκρυπτογράφηση της ψηφιακής υπογραφής και κατά συνέπεια της ανάκτησης της σύνοψης H(m) του αρχικού κειμένου m.
- Ο παραλήπτης χρησιμοποιεί τον ίδιο αλγόριθμο κατακερματισμού με τον αποστολέα, για να παράγει μια σύνοψη του μηνύματος, όπως αυτό έχει φθάσει στα χέρια του.
- Συγκρίνονται οι δύο συνόψεις, δηλαδή αυτή που δημιουργήθηκε από τον παραλήπτη, με αυτή που αποκρυπτογραφήθηκε στο πρώτο βήμα.

Οποιαδήποτε μεταβολή στα δεδομένα, θα έχει ως αποτέλεσμα τη διαφοροποίηση των συνόψεων. Με τον τρόπο αυτό ο παραλήπτης μπορεί να επιβεβαιώσει:
1) Ότι τα δεδομένα δεν έχουν μεταβληθεί κατά τη διάρκεια της επικοινωνίας.
2) Ότι το δημόσιο και το ιδιωτικό κλειδί του αποστολέα είναι πράγματι ορθό ζεύγος.

Η επαλήθευση της οντότητας αποστολής και η ακεραιότητα των δεδομένων, αν και πολύ σημαντικά στοιχεία, δεν αποδεικνύουν υποχρεωτικά την ταυτότητα του ιδιοκτήτη του δημόσιου κλειδιού. Ο παραλήπτης του μηνύματος θέλει να είναι βέβαιος ότι ο αποστολέας είναι αυτός που ισχυρίζεται ότι είναι. Ο οποιοσδήποτε θα

μπορούσε να ζητήσει την έκδοση ενός ζεύγους κλειδιού υπό άλλο όνομα και στη συνέχεια να ανακοινώσει ότι το τάδε δημόσιο κλειδί είναι δικό του. Συνεπώς ο παραλήπτης θα πρέπει να διαθέτει περισσότερες και πραγματικά αξιόπιστες πληροφορίες για τον ιδιοκτήτη του κλειδιού. Η σημαντικότερη μέθοδος στην κατεύθυνση αυτή βασίζεται στην ύπαρξη μιας έμπιστης οντότητας που ονομάζεται Αρχή Πιστοποίησης (Certification Authority, CA) και εκδίδει ψηφιακά πιστοποιητικά (certificates).
Επιπρόσθετα στις υπογραφές αυτές, που χρησιμοποιούν κρυπτογραφία δημοσίου κλειδιού, ο παραλήπτης μπορεί να αποδείξει ότι ένα μήνυμα στάλθηκε από τον αποστολέα εφόσον το ιδιωτικό κλειδί του αποστολέα παραμένει μυστικό. Αν ο αποστολέας αποκαλύψει το ιδιωτικό του κλειδί, ο καθένας θα μπορούσε να στείλει το συγκεκριμένο μήνυμα και έτσι ο παραλήπτης δε θα μπορεί να αποδείξει τίποτα. Υπάρχει όμως και το ενδεχόμενο ο αποστολέας να αποφασίσει να αλλάξει το κλειδί του. Κάτι τέτοιο είναι απόλυτα νόμιμο και συμβαίνει συχνά. Στην περίπτωση αυτή πάλι ο παραλήπτης δεν θα μπορεί να αποδείξει τίποτα, διότι θα έχει μια «παλιά ψηφιακή υπογραφή» που παράχθηκε με το παλιό κλειδί του αποστολέα. Επομένως φαίνεται και εδώ η ανάγκη ύπαρξης μιας αρχής που θα καταγράφει όλες τις αλλαγές κλειδιών και τις αντίστοιχες ημερομηνίες που έλαβαν χώρα οι αλλαγές.

ΜΕΡΟΣ 4ο

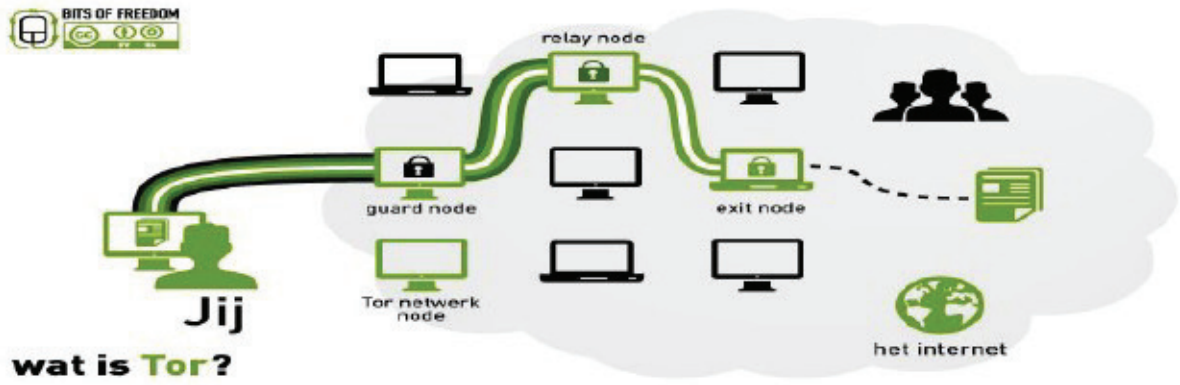
TOR (THE ONION ROUTER)

ΚΕΦΑΛΑΙΟ 8

Δρομολόγηση Onion

8.1 ΕΙΣΑΓΩΓΗ

Η δρομολόγηση onion (Onion Routing), είναι μια τεχνική για την ανώνυμη επικοινωνία σε ένα δίκτυο υπολογιστών. Το Onion Routing αποτελεί μία γενικού σκοπού υποδομή για ιδιωτικές συνδέσεις σε ένα δημόσιο δίκτυο μεταφοράς δεδομένων. Παρέχει ανώνυμες συνδέσεις χρησιμοποιώντας διαφορετικά επίπεδα κρυπτογράφησης που είναι ιδιαίτερα ανθεκτικά σε επιθέσεις τύπου ωτακουστών και ανάλυσης κίνησης. Οι συνδέσεις είναι δικατευθυντήριες, σχεδόν πραγματικού χρόνου και μπορούν να χρησιμοποιηθούν είτε για κινήσεις προσανατολισμένες σε σύνδεση, είτε για κινήσεις άνευ εγκατάστασης σύνδεσης. Το Onion Routing βασίζεται σχεδιαστικά στην ιδέα της ανάμιξης των συνδέσεων των χρηστών και των εφαρμογών, ώστε να επιτευχθεί η απόκρυψη της ταυτότητας του χρήστη σε μία επικοινωνία μέσω ενός δημόσιου δικτύου. Έτσι τελικά είναι δύσκολο να διακριθεί μία συγκεκριμένη σύνδεση. Το Onion Routing αποτρέπει εκείνους που έχουν πρόσβαση στο μέσο μετάδοσης να αναγνωρίσουν τις οντότητες που συμμετέχουν σε μία επικοινωνία, επιτρέποντάς τους μόνο να διαπιστώσουν απλώς ότι διεξάγεται κάποια επικοινωνία. Το Onion Routing παρέχει ανώνυμες συνδέσεις ανθεκτικές στην παρακολούθηση περιεχομένου της επικοινωνίας, αλλά και στην ανάλυση της κίνησης της πληροφορίας. Το Onion routing αποτελείται από δύο κύρια μέρη: τη δικτυακή υποδομή που εξυπηρετεί τις ανώνυμες συνδέσεις και περιλαμβάνει τους δρομολογητές Onion τους πληρεξούσιους που μεσολαβούν στις εφαρμογές του χρήστη και στις συνδέσεις στο Internet. Η ιδέα της δρομολόγησης onion είναι να προστατεύσει την ιδιωτικότητα του αποστολέα και του παραλήπτη του μηνύματος και, επίσης να παρέχει την προστασία του περιεχομένου του μηνύματος καθώς δρομολογείται στο δίκτυο. Η δρομολόγηση onion έχει στηριχτεί πάνω στην ιδέα των Mix Networks τα οποία δημιουργήθηκαν στις αρχές του 1980 από τον David Chaum. Ο D.Chaum είναι ο εφευρέτης πολλών κρυπτογραφικών πρωτοκόλλων στα οποία περιλαμβάνονται οι ψηφιακές υπογραφές (digital signature), η ηλεκτρονική ψηφοφορία (voting systems) και το ψηφιακό χρήμα (digital cash).

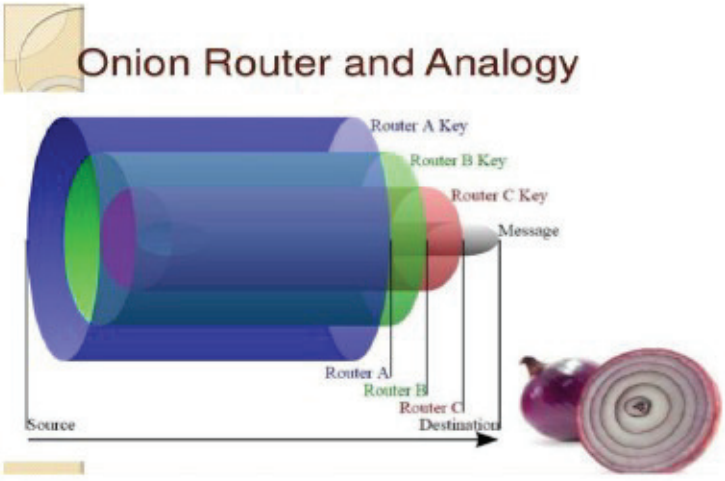


Τα mix networks δημιουργούν μια σκληρή ανιχνευσιμότητα της επικοινωνίας χρησιμοποιώντας proxy servers.Κάθε μήνυμα κρυπτογραφείται σε κάθε proxy χρησιμοποιώντας ένα δημόσιο κλειδί κρυπτογραφίας. Το αποτέλεσμα της κρυπτογράφησης είναι επίπεδο κάτι σαν την Ρώσικη κούκλα, όπου η κάθε κούκλα είναι στο ίδιο μέγεθος, και το μήνυμα να βρίσκεται στο εσωτερικό επίπεδο. Κάθε proxy server «ξεγυμνώνει» το επίπεδο κρυπτογράφησης για να αποκαλύψει που θα στείλει μετά το μήνυμα. Βασική έννοια στα mixnets είναι ο MIX, ένας proxy που αποδέχεται τα κρυπτογραφημένα μηνύματα με το public key τους τα αποκωδικοποιεί τα ταξινομεί και τα προωθεί στον τελικό αποδέκτη τους διαγράφοντας όλες τις πληροφορίες για την πηγή τους. Το πλεονέκτημα είναι, ότι, αν ένας από τους proxy servers είναι εκτεθειμένος, η ανώνυμη επικοινωνία μπορεί ακόμα να κατορθωθεί. Αυτό συμβαίνει επειδή κάθε δρομολογητής στην δρομολόγηση onion δέχεται μηνύματα, τα επανακρυπτογραφεί και τα μεταφέρει στον επόμενο δρομολογητή onion. Ένας επιτιθέμενος που έχει την ικανότητα να ελέγχει κάθε δρομολογητή σε ένα δίκτυο μπορεί να εντοπίσει την πορεία ενός μηνύματος μέσα στο δίκτυο. Όμως ένας επιτιθέμενος με περιορισμένες ικανότητες θα έχει τη δυσκολία να ανακαλύψει το μονοπάτι του μηνύματος, ακόμα και αν ελέγχει έναν ή περισσότερους δρομολογητές onion. Η δρομολόγηση onion δεν παρέχει τη τέλεια ανωνυμία του αποστολέα και του παραλήπτη ενάντια σε όλα τα πιθανά κρυφακούσματα σε ιδιωτικές συνομιλίες. Επιτρέπει έναν ισχυρό βαθμό διαχωρισιμότητας, με την ιδέα ότι ένας επιτιθέμενος δύσκολα θα ξεχωρίσει τον αποστολέα και τον παραλήπτη ενός δεδομένου μηνύματος. Ακόμη και μέσα σε αυτά τα όρια, η δρομολόγηση onion δεν παρέχει οποιαδήποτε απόλυτη εγγύηση της μυστικότητας. Αντιθέτως, παρέχει μια συνέχεια στην οποία ο βαθμός μυστικότητας είναι γενικά μια λειτουργία του αριθμού των συμμετεχόντων δρομολογητών εναντίον του αριθμού των κακόβουλων δρομολογητών. Οι δρομολογήσεις onion είναι δομές δεδομένων που χρησιμοποιούν μηνύματα για να δημιουργήσουν τις πορείες μέσω των οποίων πολλά από αυτά μπορούν να διαβιβαστούν.Τα μηνύματα που δρομολογούνται, κρυπτογραφούνται επανειλημμένα και στέλνονται μέσω διαφόρων κόμβων του δικτύου, οι οποίοι αποκαλούνται δρομολογητές onion. Οι Onion δρομολογητές συνδέονται στο δημόσιο δίκτυο, αλλά έχουν αποκαταστήσει μία και μοναδική σύνδεση με καθένα από τους γειτονικούς τους δρομολογητές Onion και μόνον έτσι μπορούν να επικοινωνούν. Σκοπός των πληρεξούσιων είναι να μεταφράζουν τα δεδομένα σε μορφή ανεξάρτητη της εκάστοτε εφαρμογής, η οποία θα γίνεται αποδεκτή και κατανοητή από το δίκτυο των δρομολογητών Onion. Κάθε δρομολογητής onion, ο οποίος γνωρίζει την ταυτότητα και τα δημόσια κλειδιά των υπόλοιπων δρομολογητών, αφαιρεί ένα στρώμα της κρυπτογράφησης για να αποκαλύψει τις οδηγίες δρομολόγησης και στέλνει το μήνυμα στον επόμενο δρομολογητή, όπου αυτό επαναλαμβάνεται έως ότου το μήνυμα φτάσει στον τελικό προορισμό του. Ο Onion πληρεξούσιος που βρίσκεται στην πλευρά του αποστολέα, επιλέγει ένα μονοπάτι από το οποίο θα φτάσει στον παραλήπτη. Αυτή η διαδικασία αποτρέπει τους ενδιάμεσους κόμβους να γνωρίζουν την προέλευση, τον προορισμό και το περιεχόμενο του μηνύματος. Κατά μήκος του μονοπατιού υπάρχουν και άλλοι δρομολογητές. Για κάθε δρομολογητή,

στο μονοπάτι που επιλέχτηκε, δημιουργείται ένα στρώμα με ένα πακέτο που περιλαμβάνει την IP διεύθυνση του επόμενου δρομολογητή και τις πληροφορίες που απαιτούνται για τη δημιουργία του κλειδιού κρυπτογράφησης. Αυτό το στρώμα με το πακέτο θα χρειαστεί ώστε να είναι σε θέση να επικοινωνήσει με τον επόμενο. Τα πακέτα αυτά, αντί να μεταφέρουν πληροφορία για την πηγή και τον προορισμό τους, περιέχουν πληροφορία μόνο για τον προηγούμενο και τον επόμενο σταθμό. Επομένως, στον αμέσως επόμενο από το χρήστη δρομολογητή δημιουργείται ένα Onion, το οποίο καθορίζει το μονοπάτι της σύνδεσης στο Internet. Κατά τη χρησιμοποίηση της δρομολόγησης onion η αλυσίδα των κόμβων διαμορφώνεται ως εξής: ο ιδρυτής κρυπτογραφεί τα στοιχεία που θέλει να επικοινωνήσει σε διάφορα layers με την ενίσχυση της βασικής κρυπτογράφησης δημόσιου κλειδιού και το στέλνει στον πρώτο κόμβο. Ο κόμβος εισόδου θα αφαιρέσει το πρώτο στρώμα της κρυπτογράφησης και θα μεταλλάξει τα στοιχεία ο δεύτερος κόμβος. Εκείνος ο κόμβος θα αφαιρέσει επίσης ένα στρώμα της κρυπτογράφησης και θα στείλει στοιχεία στον τρίτο κόμβο. Κάθε διαδοχικός κόμβος θα κάνει επιπλέον αυτή τη διαδικασία μέχρι τον τελευταίο κόμβο, όπου ο κόμβος εξόδου θα αφαιρεί το υπόλοιπο στρώμα της κρυπτογράφησης και στέλνει το αποκρυπτογραφημένο μήνυμα στον προοριζόμενο παραλήπτη. Κάθε μεμονωμένος κόμβος ξέρει μόνο την ταυτότητα και τη διεύθυνση IP του προηγούμενου και του διαδοχικού κόμβου. Και μόνο ο κόμβος εξόδου και εισόδου αντίστοιχα ξέρει τον ιδρυτή και τον προοριζόμενο παραλήπτη της επικοινωνίας. Αυτό σημαίνει ότι είναι πιθανό να συσχετίσουν την πλήρη επικοινωνία εφ' όσον υπάρχουν το λιγότερο τρεις κόμβοι. Εφ' όσον αλλάζει αυτή η αλυσίδα αρκετά συχνά, ή ο ιδρυτής είναι μέρος μιας αλυσίδας άλλου χρήστη, η δρομολόγηση onion παρέχει μια πολύ υψηλότερου επιπέδου ανωνυμία από ότι άλλες τεχνολογίες ιδιωτικότητας, επειδή ο βαθμός του εγκυρότητας ενός χρήστη μειώνεται σημαντικά.

8.2 ΑΡΧΕΣ ΛΕΙΤΟΥΡΓΙΑΣ TOR

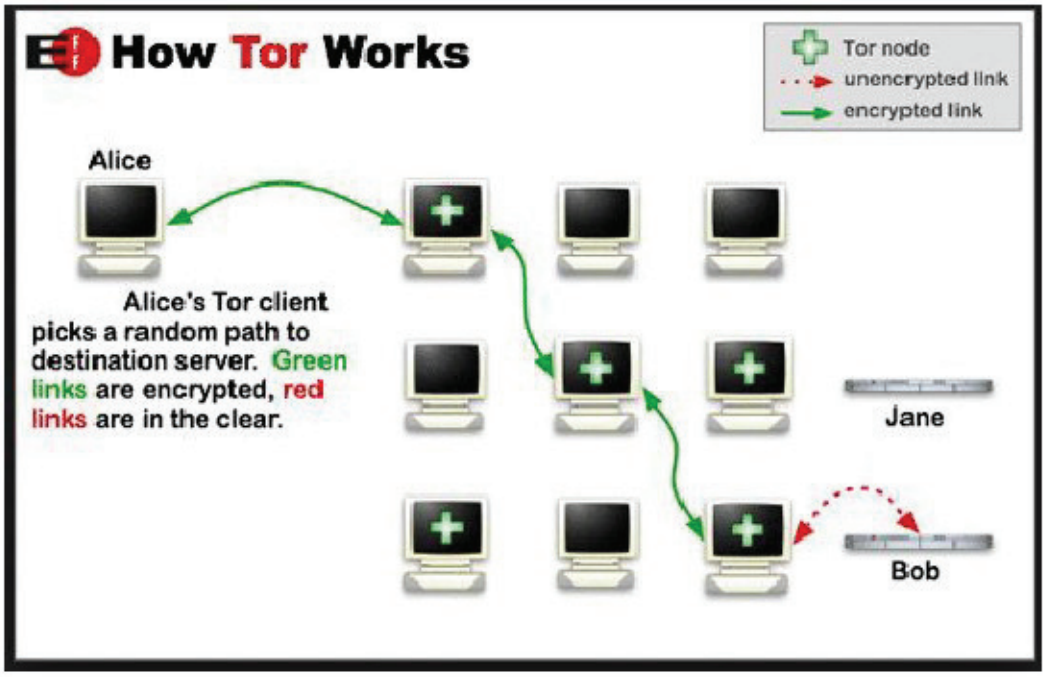
Η πλήρης ονομασία του είναι: The Onion Router (Tor) και πρωτοδημιουργήθηκε πριν κάποια χρόνια για τις ανάγκες του ναυτικού των ΗΠΑ. Η λέξη onion (=κρεμμύδι) υποδηλώνει τα πολλαπλά "στρώματα" που χρησιμοποιεί κατά την λειτουργία του.



Το Tor (συντομογραφία του The onion router) είναι ένα σύστημα που δίνει στους

χρήστες του τη δυνατότητα ανωνυμίας στο Διαδίκτυο. Αυτό το καταφέρνει καθοδηγώντας την ανταλλαγή δεδομένων μέσα από ένα χαοτικό δίκτυο πολλών διαμεσολαβητών υπολογιστών (proxy servers), τους οποίους τρέχουν διάφοροι εθελοντές, οπότε ο καθένας μπορεί να αποτελέσει μέρος του δικτύου. Η πρώτη έκδοση του λογισμικού ανακοινώθηκε στις 20 Σεπτεμβρίου του 2002 από τους δημιουργούς του Roger Dingledine και Nick Mathewson .Σκοπός του Tor είναι να "κρύψει" την ταυτότητα του χρήστη και τις ενέργειές του ώστε να μην φαίνεται σ' αυτούς που τους παρακολουθούν ποιες ιστοσελίδες επισκέπτονται, τι δραστηριότητες έχουν και με ποιους επικοινωνούν .Η χρήση του Tor κάνει δύσκολη την ανίχνευση διαδικτυακής δραστηριότητας του χρήστη καθώς τα δεδομένα που ανταλάσσονται κινούνται κρυπτογραφημένα σε τυχαίες διαδρομές τις οποίες κανένας υπολογιστής του δικτύου δεν γνωρίζει ολόκληρες, ώστε να μην μπορεί να εξακριβώσει την προέλευση ή τον προορισμό των δεδομένων. Κάθε δέκα λεπτά περίπου , δημιουργείται ένα καινούριο κύκλωμα διαμεσολαβητών , το οποίο έχει και διαφορετικό διαμεσολαβητή εξόδου, οπότε παρέχει και μια διαφορετική IP στο δίκτυο. Πιο συγκεκριμένα τα δεδομένα και ο τελικός προορισμός κρυπτογραφούνται (με τη χρήση δημοσίου κλειδιού) πριν πάνε από τον υπολογιστή στον διαμεσολαβητή-κόμβο εισόδου και δημιουργείται ένα κρυπτογραφημένο κανάλι επικοινωνίας.Μέσα από αυτό το κανάλι δημιουργείται μια αντίστοιχη σύνδεση με έναν τυχαίο ενδιάμεσο κόμβο του δικτύου, ο οποίος στέλνει και αυτός το δημόσιο κλειδί του στον υπολογιστή του χρήστη. Με αυτόν τον τρόπο δημιουργούνται κρυπτογραφημένα κανάλια μέσα από τα προηγούμενα κανάλια , χωρίς όμως να έχουν τη δυνατότητα να αποκρυπτογραφήσουν τον προορισμό ή τα δεδομένα. Όλη η διαδικασία μοιάζει με κρεμμύδι γιατί έχει πολλαπλά στρώματα (κανάλια), εξού και το όνομα (onion). Το ίδιο ισχύει και για την αποκρυπτογράφηση του μηνύματος και την επικοινωνία με τον κόμβο εξόδου.Ο κόμβος εξόδου όμως μπορεί να αποκρυπτογραφήσει τα αρχικά δεδομένα αλλά όχι την προέλευση τους.Για αυτό το λόγο κάποιοι χρησιμοποιούν τους κόμβους εξόδου του Tor σαν «ωτακουστές» και με αυτή τη μέθοδο έχουν διαρρεύσει στο παρελθόν ευαίσθητες πληροφορίες και διπλωματικές επικοινωνίες των ΗΠΑ στο wikileaks. Οι χρήστες του δικτύου Tor τρέχουν στον υπολογιστή τους έναν διακομιστή μεσολάβησης (proxy). Η αυτονομία της εφαρμογής του Tor το καθιστά διαφορετικό από τα περισσότερα δίκτυα ανωνυμοποίησης καθώς λειτουργεί στο Transmission Control Protocol (TCP) επίπεδο μεταφοράς OSI. Στις εφαρμογές που χρησιμοποιούν ευρέως το Tor για ανωνυμοποίηση περιλαμβάνονται το Internet Relay Chat (IRC),όπως και προγράμματα άμεσων μηνυμάτων και στην περιήγηση στο World Wide Web. Όταν πραγματοποιείται περιήγηση στο διαδίκτυο, το Tor συχνά συνδυάζεται με τη χρήση των διακομιστών μεσολάβησης Polipo ή Privoxy.Ένα ακόμη από τα πλεονεκτήματά του είναι ότι στις τελευταίες εκδόσεις το Tor παρέχει το δικό του επιλυτή (Domain Name System) DNS ο οποίος θωρακίζει το χρήστη από ανεπιθύμητη παρακολούθηση όπως για παράδειγμα ο καθορισμός των www ιστοσελιδών που επισκέπτεται.Ένα εύλογο ερώτημα είναι αν και γιατί αξίζει να το εμπιστευτούμε καθώς ένας proxy server μπορεί να υποκλέπτει και να προδώσει την

ταυτότητά μας σκόπιμα.Σίγουρα δεν μπορούμε να είμαστε σίγουροι για τις προθέσεις των δημιουργών όμως το ότι το Tor είναι ενα εργαλείο ανοιχτού κώδικα και ελεύθερου λογισμικού το καθιστά έμπιστο και δίνει την δυνατότητα σε μεγάλος μέρος προγραμματιστών να εξετάσει, να συγκρίνει τον κώδικα με αυτόν της σελίδας του Tor ή και να καλύψει κενά ασφαλείας.Έτσι το λογισμικό είναι ασφαλές και συνεχώς ενημερωμένο.



8.3 ΑΔΥΝΑΜΙΕΣ ΔΙΚΤΥΟΥ TOR

Όπως όλα τα τωρινά δίκτυα ανωνυμοποίησης χαμηλής λανθάνουσας, το Tor δεν μπορεί και δεν προσπαθεί να προστατεύσει τους χρήστες από την παρακολούθηση της κίνησης στα όρια του δικτύου Tor, όπως για παράδειγμα, η κίνηση που εισέρχεται και εξέρχεται από το δίκτυο. Ενώ το Tor παρέχει προστασία κατά της ανάλυσης κίνησης, δεν προλαμβάνει την επιβεβαίωση της κίνησης (ονομάζεται. επίσης. από άκρη σε άκρη συσχετισμός). Τον Μάρτιο του 2011, ερευνητές μαζί με ανθρώπους από το Rocquencourt, το εθνικό ινστιτούτο έρευνας στην επιστήμη της πληροφορικής και του ελέγχου (Institut national de recherche en informatique et en automatique, INRIA), που βρίσκεται στην Γαλλία, κατέγραψαν μια επίθεση ικανή να αποκαλύψει τη διεύθυνση IP των χρηστών του BitTorrent στο δίκτυο Tor. Η επίθεση bad apple χρησιμοποιεί τον σχεδιασμό του Tor και εκμεταλλεύεται κάθε μη ασφαλή χρήση εφαρμογής για να συσχετίσει την ταυτόχρονη χρήση μιας ασφαλής εφαρμογής με την διεύθυνση IP του συγκεκριμένου χρήστη Tor. Μία μέθοδος επίθεσης εξαρτάται από τον έλεγχο ενός κόμβο εξόδου ή την υποκλοπή της απάντησης ενός ανιχνευτή, ενώ μία δεύτερη μέθοδος επίθεσης βασίζεται εν μέρει στην στατιστική εκμετάλλευση της

ανίχνευσης του κατανεμημένου πίνακα κατακερματισμού.

Τον Οκτώβριο του 2011 ερευνητική ομάδα από την Esiea, Γαλλική σχολή μηχανολόγων, δήλωσε ότι ανακάλυψε έναν τρόπο να υπονομεύσει το δίκτυο του Tor με το να αποκρυπτογραφήσει επικοινωνίες που το διαπερνούν. Η τεχνική που περιέγραψαν απαιτεί τη δημιουργία ενός χάρτη των κόμβων του δικτύου Tor, τον έλεγχο του ενός τρίτου από αυτούς και στην συνέχεια να αποκτήσουν τα κλειδιά κρυπτογράφησής τους και τις πηγές του αλγόριθμου. Ύστερα, χρησιμοποιώντας τα γνωστά πλέον κλειδιά και τις πηγές θεωρούν ότι έχουν την ικανότητα να αποκρυπτογραφούν δύο από τα τρία στρώματα κρυπτογράφησης. Ισχυρίζονται ότι μπορούν να σπάσουν το τρίτο κλειδί με μια επίθεση που βασίζεται στην στατιστική ανάλυση. Για να επανακατευθύνουν την κίνηση του Tor στους κόμβους που ελέγχουν, χρησιμοποίησαν μεθόδους επίθεσης άρνησης εξυπηρέτησης και επίθεσης packet spinning. Καμία τεχνική ανάλυση δεν είναι ακόμα διαθέσιμη για το κοινό ή για του κατασκευαστές του Tor για περαιτέρω μελέτη.

Στη συνέχεια αναφέρονται οι αδυναμίες του TORκαι οι μορφές επίθεσης που μπορεί να δεχτεί η ασφάλεια και η ανωνυμία του

- Ταυτοποίηση κίνησης: Αν κάποιος παρακολουθεί τη σύνδεση δικτύου του υπολογιστή (και δεν τον έχει παγιδέψει με spyware), μπορεί να καταλάβει ότι χρησιμοποιείται tor, αλλά δεν μπορεί να διαβάσει τις κρυπτογραφημένες ροές και να δει τη δραστήριότητά του. Μπορεί όμως να μετρήσει τον όγκο των δεδομένων του και το χρόνο εκπομπής τους, δεδομένου ότι πρόκειται για σύστημα χαμηλής καθυστέρησης. Έτσι, αν με κάποιο τρόπο υποθέσει ποιός είναι ο κόμβος εξόδου, μπορεί να κάνει την ταυτοποίηση κίνησης. Στην πράξη βέβαια η χαοτικότητα του tor προστατεύει αποτελεσματικά από την ταυτοποίηση κίνησης, καθώς είναι πολύ δύσκολο να υποθέσεις και να συγκρίνεις σε τόσο μεγάλο πλήθος κόμβων εξόδου. Αντίστοιχη δυσκολία υπάρχει στο να ταυτοποιήσουν τον κόμβο εισόδου (άρα και τη θέση του υπολογιστή) αν γνωρίζουν τον κόμβο εξόδου (απ' τον οποίο π.χ. στάλθηκε μια ανάληψη ευθύνης). Η επίθεση αυτή δεν είναι εφικτή αν χρησιμοποιείται το εσωτερικό διαδίκτυο του tor, που οι σελίδες του έχουν κατάληξη .onion και δεν είναι ορατές από το εκτός του tor διαδίκτυο.
Ένας τρόπος άμυνας σε αυτήν την επίθεση είναι η εισαγωγή χαοτικών δεδομένων. Το tor δεν ενσωματώνει αυτήν την τεχνική για να μην επιβαρύνει το δίκτυό του, δίνει όμως μια αρκετά καλύτερη επιλογή, να τρέξει έναν ενδιάμεσο relay server, πράγμα που ισοδυναμεί με ροή τυχαίων δεδομένων και αντί να επιβαρύνει το δίκτυο το ενισχύει.
- Κατάληψη μέρους του δικτύου: Αν κάποιος που θέλει να σπάσει την ανωνυμία του χρήστη , τρέχει αρκετούς κόμβους εισόδου και εξόδου, είναι πιθανό να τύχει να χρησιμοποιεί ονχρήστης μαζί, τους δικούς του διαμεσολαβητές, οπότε να καταφέρει να ταυτοποιηθεί ο χρήστηςΕπειδή όμως στατιστικά είναι πολύ μικρή η πιθανότητα να λειτουργήσει αποτελεσματικά κάτι τέτοιο με λίγους διαμεσολαβητές, χρειάζεται να καταληφθεί περίπου το ένα τρίτο

του δικτύου. Στην πράξη δεν υπάρχουν ενδείξεις για παρόμοιο εγχείρημμα.

- Επίθεση στην κρυπτογραφία: Το σπάσιμο των κωδικών είναι ζήτημα υπολογιστικής ισχύος. Οι υπερυπολογιστές που υπάρχουν σήμερα δεν επαρκούν για την αποκρυπτογράφηση, όμως οι ροές καταγράφονται από την NSA (National Security Agency) και πιθανόν άλλες μυστικές υπηρεσίες και κάποια στιγμή στο μέλλον θα τις αποκρυπτογραφήσουν. Ότι μεταφέρουμε σήμερα, η θέση και η ταυτότητά μας θα αποκαλυφθεί στο μακρινό μέλλον. Τότε όμως θα έχει εξελιχθεί και το tor. Ήδη συζητιέται στην κοινότητα ανάπτυξης του tor ο διπλασιασμός του μεγέθους των κωδικών κρυπτογράφησης.
- Επίθεση άρνησης εξυπηρέτησης: Αρκετά διαδεδομένη στο ίντερνετ (denial of service, dos). Ουσιαστικά είναι η υπερφόρτωση ενός σέρβερ από μαζικές αιτήσεις που γίνονται αυτόματα από προγράμματα γι αυτό το σκοπό (bots), ώστε να μην μπορεί να λειτουργήσει. Τελευταία το δίκτυο του tor δέχεται τέτοιου είδους επιθέσεις, με αποτέλεσμα να παρουσιάζει πρόβλημα στην χρηστικότητά του καθώς σέρνεται. Δεν πρόκειται όμως για αποκάλυψη της ανωνυμίας. Μπορεί όμως θεωρητικά να χρησιμοποιηθεί συνδυαστικά με την κατάληψη μέρους του δικτύου, διοχετεύοντας επιθέσης άρνησης εξυπηρέτησης στοχευμένα ενάντίον των υπόλοιπων διαμεσολαβητών ώστε να αναγκαστεί ο χρήστης να συνάψει κύκλωμα με τους διαμεσολαβητές υποκλοπείς.
- Επίθεση σε περιφερειακό του tor λογισμικό: Όπως είδαμε παραπάνω, εάν ο υπολογιστής του χρήστη είναι παγιδευμένος με κατασκοπευτικό λογισμικό, κανένα δίκτυο ανωνυμίας δε σε προστατεύει. Οπότε ο υπολογιστής πρέπει να είναι καθαρός. Το κυριότερο αν κάποιος είναι στόχος παρακολούθησης είναι η επιλογή του λειτουργικού συστήματος.

Όμως υπάρχουν και άλλα υποσυστήματα με τα οποία συνεργάζεται το tor και από τα οποία μπορεί κάποιος να προδωθεί. Για παράδειγμα το υποσύστημα DNS (Domain Name System, το σύστημα που μεταφράζει τις διευθύνσεις των ιστοσελίδων τύπουhttp://www.xxxxxxx.xxx στις κατάλληλες IP διευθύνσεις των σελίδων), πριν ενσωματωθεί στο tor, ζητούσε κανονικά τις σελίδες που επισκεπτόμασταν μέσω tor, με αποτέλεσμα κάποιος που μας παρακολουθεί να μπορεί να συναγάγει ποιές σελίδες επισκεφθήκαμε (όχι όμως τί κάναμε).

Πλέον το tor έχει καλύψει αυτήν την τρύπα ασφαλείας περνόντας τα αιτήματα DNS μέσα από το δίκτυό του.

Πάντως αν μαζί με το tor χρησιμοποιείται ελαττωματικό λογισμικό και μία ισχυρή αστυνομική υπηρεσία όπως το FBI ή η NSA θέλει να εντοπίσει κάποιον χρήστη , αυτό είναι εύκολο.. Μία τέτοια περίπτωση είναι η πρόσφατη σύλληψη από το FBI ενός διακινητή παιδικής πορνογραφίας. Στην περίπτωση αυτή, χάκαραν κάποιες .onion ιστοσελίδες (μεταξύ των οποίων και το δημοφιλές tormail) , ώστε όταν εκτελέσουν κακόβουλο κώδικα όταν ανοίξουν στον tor-browser για windows, και να στείλουν σήμα εκτός του tor δικτύου, σε κάποιο σέρβερ της αστυνομίας στη Βιρτζίνια ώστε να εντοπισουν τους χρήστες. Για να σπάσει δηλαδή το FBI την ισχυρή ανωνυμία που προσφέρει το tor-network, εκμεταλλεύτηκαν συνδυασμό από αδυναμίες στο περιφερειακό του tor λογισμικό tor-browser, στην ελαττωματική

υποδομή ασφαλείας του λειτουργικού συστήματος ms windows, και στις ιστοσελίδες που χάκαραν. Έτσι αρκετοί χρήστες του tor αποκαλύφθηκαν όταν έλαβε χώρα η επίθεση. Όχι όλοι όμως. Όσοι δεν επισκέφθηκαν τις χακαρισμένες σελίδες δεν προσβλήθηκαν. Επίσης, όσοι χρησιμοποιούσαν άλλο λειτουργικό σύστημα (osx ή gnu linux) επίσης δεν έπαθαν τίποτα. Άμεσα κυκλοφόρησε ανανεωμένη έκδοση του tor-browser για windows που διόρθωνε αυτήν την αδυναμία. Το μεγαλύτερο πλήγμα απ' αυτήν την επίθεση, ήταν στην υπόληψη του tor-project, που είχε ως αποτέλεσμα πολλοί χρήστες του λόγω άγνοιας να στραφούν σε πιο επισφαλείς λύσεις ανωνυμίας, με τη συνακόλουθη μείωση της χαοτικότητας του, που είναι και η πηγή της δύναμής του.

8.4 ΘΩΡΑΚΙΣΗ ΤΗΣ ΑΝΩΝΥΜΙΑΣ ΣΤΗΝ ΠΡΑΞΗ

Tor browser bundle

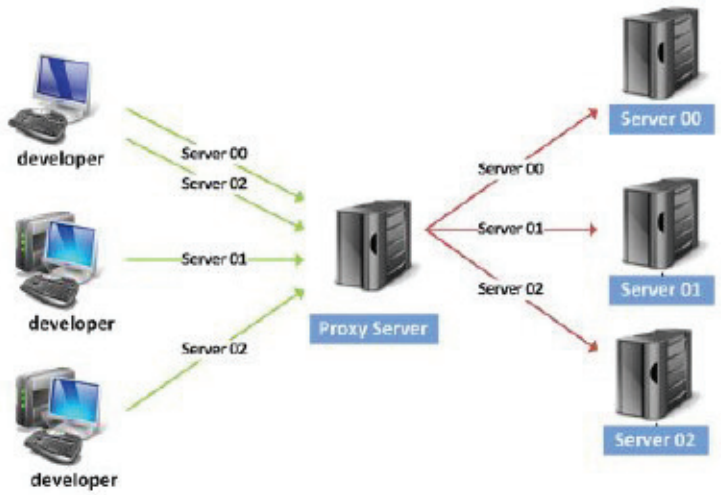
Στην ιστοσελίδα του tor προσφέρονται διάφορα προγράμματα-εργαλεία για κάθε χρήση του tor network και για όλα τα διαδεδομένα λειτουργικά συστήματα. Το πιο δημοφιλές και εύχρηστο εργαλείο είναι το tor-browser bundle, ένα πακέτο προγραμμάτων που περιλαμβάνει το vidallia που πραγματοποιεί αυτόματα την κατάλληλη ρύθμιση του υπολογιστή, τη σύνδεση στο tor και τον tor-browser για σερφάρισμα διασφαλίζοντας την ανωνυμία, με την προυπόθεση ότι γίνεται ευφυής χρήση (δεν συνδέεσαι για παράδειγμα στο λογαριασμό σου στο facebook με τα πραγματικά σου στοιχεία). Ο browser που χρησιμοποιείται στο bundle είναι ο firefox με επιπρόσθετες ρυθμίσεις ανωνυμίας και με προεγκατηστεμένο το πρόσθετο noscript που απογορεύει την εκτέλεση κώδικα απ' τις ιστοσελίδες, ώστε να αποφευχθούν επιθέσεις . Ο χρήστης μπορεί αν θέλει να άρει τον αποκλεισμό για τις σελίδες που εμπιστεύεται. Όταν γίνει κάποια επίθεση , η προεπιλεγμένη πολιτική απαγόρευσης του noscript είχε "χαλαρώσει" ώστε να γίνει πιο χρηστικό. Η επίθεση λειτουργεί μόνο στα windows αλλά στο μέλλον πιθανό να μεταφερθεί και σε mac, android, και

κάποιες linux πλατφόρμες.

T.A.I.L.S.

Υπάρχει όμως μία διανομή linux που ήταν είναι και οπως δείχνουν όλα θα παραμείνει απρόσβλητη σε τέτοιου είδους επιθέσεις: Το T.A.I.L.S. (The Amnestic Incognito Live System), 100% ελεύθερο λογισμικό. Η συγκεκριμένη διανομή, βρίσκεται ακολουθώντας link από το site του tor στον υπολογιστή,. Τρέχει χωρίς εγκατάσταση, και δεν αφήνει ίχνη στον σκληρό δίσκο (είναι το ιδανικό σύστημα για αναλήψεις ευθύνης και άλλες παράνομες δραστηριότητες).
Είναι ρυθμισμένη ώστε να μην επιτρέπει συνδέσεις εκτός του δικτύου tor και εκεί έγκειται και η θωράκισή της. Οπότε είναι εντελώς μη χρηστική για κανονικό σερφάρισμα, αλλά παντοδύναμη όσον αφορά την ανωνυμία, με περιοριστικά πρόσθετα όπως το noscript να είναι σχεδόν άχρηστα. Το σημαντικότερο, είναι σχεδόν αδύνατη η εγκατάσταση spyware.
Επίσης διαθέτει και άλλα χαρακτηριστικά όπως metadata cleaner, ένα πρόγραμμα που σβήνει τα metadata (δεδομένα που ενσωματώνονται στα αρχεία και δείχνουν ώρα και ημερομηνία κατασκευής όπως και στοιχεία του υπολογιστή στον οποίο κατασκευάστηκαν) από προυπάρχοντα αρχεία, απαραίτητο αν θέλει κάποιος να στείλεις ανώνυμα κάποιο αρχείο (π.χ. pdf).
Άλλες περιπτώσεις εσφαλμένης χρήσης απ’ τις οποίες το t.a.i.l.s. προστατεύει αποτελεσματικά είναι το άνοιγμα αρχείων που κατέβηκαν μέσω tor και ανοίγουν σε εξωτερικές εφαρμογές και μπορεί να τρέξουν σε αυτές κακόβουλο κώδικα που σε ταυτοποιεί. Στο tails αυτό δεν μπορεί να συμβεί καθώς δεν επιτρέπονται μη tor συνδέσεις από το firewall.

8.5 PROXY SERVER



Ο Proxy server, είναι ένας διακομιστής μεσολάβησης στα ελληνικά που έχει στόχο να βελτιώσει την ταχύτητα πλοήγησης στο διαδίκτυο και παράλληλα να μειώσει την κίνηση του δικτύου προς το διαδίκτυο. Τοποθετείται ενδιάμεσα των χρηστών και του διαδικτύου. Λαμβάνει τα αιτήματα ιστοσελίδων από έναν χρήστη, προσκομίζει τη σελίδα από το Διαδίκτυο, και έπειτα την δίνει στον υπολογιστή που την ζήτησε. Ο proxy server μπορεί να είναι και μέρος ενός firewall και μπορεί να αποτρέπει τους διάφορους επιτήδειους από το να χρησιμοποιήσουν το διαδίκτυο για να αποκτήσουν πρόσβαση σε υπολογιστές ενός ιδιωτικού δικτύου.
Σε ένα εσωτερικό δίκτυο ένας υπολογιστής (proxy server) συνδέεται στο Internet και παρέχει πρόσβαση στο web σε όλους τους υπόλοιπους υπολογιστές του δικτύου. Αυτό κατά βάση εξυπηρετεί τον σκοπό της κεντρικής διαχείρισης της πρόσβασης στο web. Συνεπώς μέσω του proxy server μπορούμε να επιτρέψουμε ή να απαγορεύσουμε την πρόσβαση στο web σε κάθε έναν υπολογιστή του δικτύου ξεχωριστά, κάτι ιδιαίτερα χρήσιμο σε εταιρικά περιβάλλοντα. Το σύστημα αυτό συνοπτικά λειτουργεί με τον ακόλουθο τρόπο:
Ο υπολογιστής (client) που θέλει να συνδεθεί με μία δικτυακή τοποθεσία προωθεί την διεύθυνσή της (URL) στον proxy server. Αυτός συνδέεται στην διεύθυνση που ζητήθηκε, παίρνει το περιεχόμενό της και το προωθεί στον client. Έτσι ο client, παρότι ο ίδιος δεν έχει άμεση πρόσβαση στο Internet μπορεί να βλέπει ιστοσελίδες μέσω του proxy server.
Ο proxy είναι στην ουσία, μια μεγάλη cache και οι servers που παρέχουν αυτές τις υπηρεσίες είναι πολύ ισχυρά μηχανήματα, με μεγάλο και γρήγορο σκληρό δίσκο. Όταν ο χρήστης ζητάει μια σελίδα από το Internet, αυτό το αίτημα, διαβιβάζεται στον proxy.
Αν την σελίδα την έχει αποθηκευμένη στην μνήμη του ο proxy, την δίνει απευθείας στον browser και δεν χρειάζεται να την ζητήσει από τον Web server με όλη την καθυστέρηση που συνεπάγεται αυτό για τον χρήστη (στην περίπτωση αυτή, η μόνη επικοινωνία του proxy με τον Web server που φυλάει την πρωτότυπη σελίδα, είναι

μια σύντομη σύνδεση για να ελέγξει αν το αντίγραφο που έχει ο proxy στην μνήμη του είναι το ίδιο με το πρωτότυπο).
Μάλιστα, οι proxy servers έχουν ανεπτυγμένες τεχνικές πρόβλεψης ζήτησης μίας σελίδας με αποτέλεσμα οι πιο συχνά χρησιμοποιούμενη πληροφορία να υπάρχει στην μνήμη του proxy server εκτός από τον δίσκο του, με αποτέλεσμα να έχουμε ακόμα γρηγορότερες αποκρίσεις. Επιπλέον, όταν ο χώρος που είναι διαθέσιμος για αποθήκευση γεμίσει και πρέπει να διαγραφούν από τον δίσκο κάποια αρχεία ώστε να δημιουργηθεί χώρος για νέα δεδομένα τότε, οι proxy servers ακολουθούν ανεπτυγμένες πολιτικές (flash policies) για την διαγραφή της λιγότερο πιθανής για ζήτηση πληροφορίας.
Τελικά, η χρήση ενός caching proxy server, παρόλο που προορίζεται κυρίως για εταιρικά περιβάλλοντα με πολλούς υπολογιστές που χρειάζονται πρόσβαση στο web, μπορούν να επιταχύνουν σημαντικά την περιήγησή μας στο Internet ακόμα και όταν πρόκειται για τον ένα και μοναδικό υπολογιστή .

Η χρήση διακομιστών μεσολάβησης (proxy servers) είναι ευρύτατη στο internet για πολλούς λόγους. Σχεδόν όλοι οι οργανισμοί ανά τον κόσμο, οι οποίοι χρησιμοποιούν εσωτερικά τοπικά δίκτυα τα οποία παρέχουν πρόσβαση στο internet, χρησιμοποιούν proxy servers. Τα πλεονεκτήματα είναι πολλά και δεν είναι εύκολο να περιγραφούν αναλυτικά σε μια ενημερωτική σελίδα, είναι όμως σκόπιμο να αναφέρουμε ότι με τους proxy επιτυγχάνουμε κατά βάση τα εξής:

Επιτάχυνση της περιήγησης στο διαδίκτυο. Ο proxy server σε όλα τα δίκτυα είναι εγκατεστημένος σε σημείο κατάλληλο ώστε να έχει την ταχύτερη πρόσβαση στο internet. Όταν ένας χρήστης χρησιμοποιεί τον proxy, ζητάει με το πρόγραμμά του την αναμετάδοση του περιεχομένου που επιθυμεί. Ο proxy πραγματοποιεί τη σύνδεση για λογαριασμό του χρήστη και αναμεταδίδει το περιεχόμενο σε αυτόν, χωρίς να πρέπει να συνδεθεί ο χρήστης με τον απομακρυσμένο τόπο μεσω γραμμών χαμηλής ταχύτητας.

Αποθήκευση των δημοφιλών σελίδων. Ο proxy όταν αναμεταδίδει ένα δικτυακό τόπο, τον αποθηκεύει και τοπικά. Ετσι, ο επόμενος χρήστης που θα θελήσει να δεί την ίδια σελίδα, την διαβάζει κατευθείαν από τον proxy server και δεν χρειάζεται να την ξαναζητήσει μέσω του internet. Ο διακομιστής μεσολάβησης ταυτόχρονα ελέγχει σε τακτά χρονικά διαστήματα για νεώτερες εκδόσεις των σελίδων. Έτσι πέραν της επιτάχυνσης, επιτυγχάνεται και απελευθέρωση της γραμμής με το internet από άσκοπες μεταφορές δεδομένων. Ενας καλός proxy server σε ένα τυπικό δίκτυο επιτυγχάνει βελτίωση μέχρι και 40%.

Αύξηση ασφάλειας από ιούς. Ο διακομιστής μεσολάβησης πέρα από την αναμετάδοση μπορεί να χρησιμοποιεί και προγράμματα ελέγχου για ιούς. Έτσι αποφεύγεται η μεταφορά επικίνδυνου περιεχομένου στους χρήστες.

Αύξηση ασφάλειας δικτύου. Οι διακομιστές μεσολάβησης είναι ισχυροί

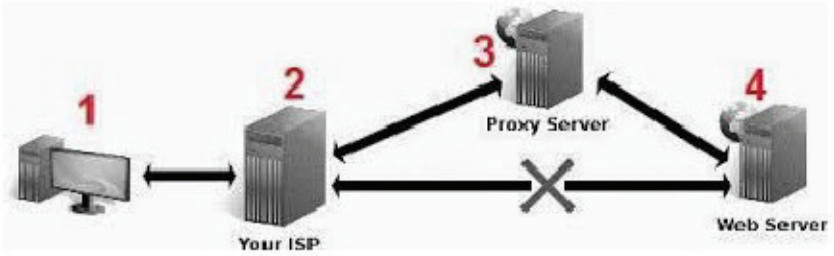
υπολογιστές με ασφαλή και σταθερά λειτουργικά συστήματα, τα οποία μέσω της λειτουργίας τους σαν proxy εμποδίζουν την απευθείας σύνδεση των χρηστών με το internet.

Ελεγχος ροής. Με τους διακομιστές μεσολάβησης, μπορούν να εφαροστούν πολιτικές που δίνουν πρωτεραιότητα στην περιήγηση στο διαδίκτυο, έναντι άλλων υπηρεσιών λιγότερο σημαντικών. Έτσι μπορεί να βελτιωθεί ακόμα περισσότερο η όλη ταχύτητα περιήγησης.

8.5.1 ΤΥΠΟΙ PROXY SERVER

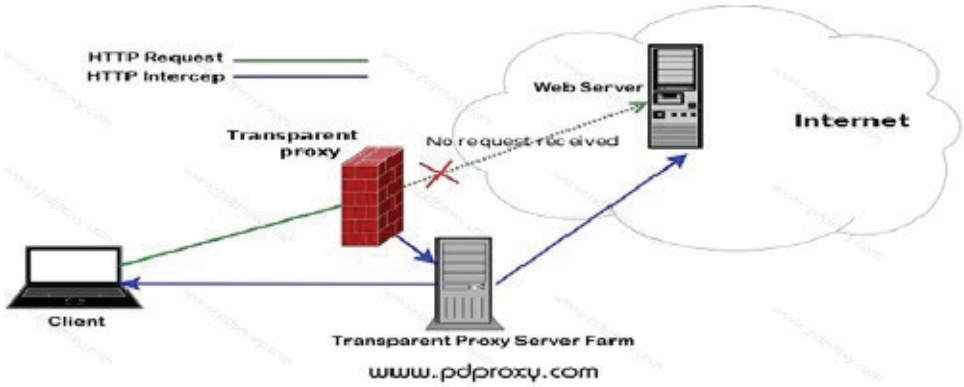
Υπάρχουν 3 είδη απο διαφορετικούς Proxy Servers. Ο κανονικός και κλασικός proxy server, ο transparent όπως λέγεται όπου κρύβει την μια πλευρά της σύνδεσης και τέλος ο reverse που κάνει κάτι τελείως διαφορετικό σε σχέση με τους άλλους δυο .

Κανονικός Proxy Server



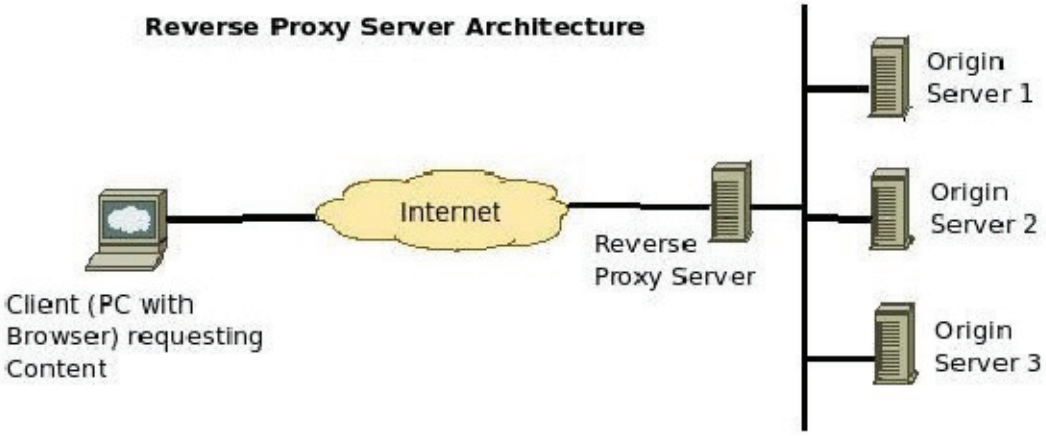
Ακούει σε μια συγκεκριμένη θύρα οπότε όλες οι αιτήσεις των χρηστών(browsers) είναι ρυθμισμένες να στέλνονται σε αυτή τη θύρα. Έπειτα ο server δέχεται την αίτηση και αποθηκεύει τα δεδομένα για μελλοντική χρήση. Όταν αργότερα έρθει άλλη μια αίτηση ζητώντας τα ίδια αρχεία με την πρώτη δεν ξανά φέρνει τα αρχεία απο την σελίδα αλλά τα έχει ήδη έτοιμα. Οπότε πολύ απλά τα δίνει στον δεύτερο χρήστη. Με αυτόν τον τρόπο μειώνεται η ταχύτητα και ο χρήστης λαμβάνει πολύ πιο γρήγορα την σελίδα του στον browser.

Transparent Proxy Server



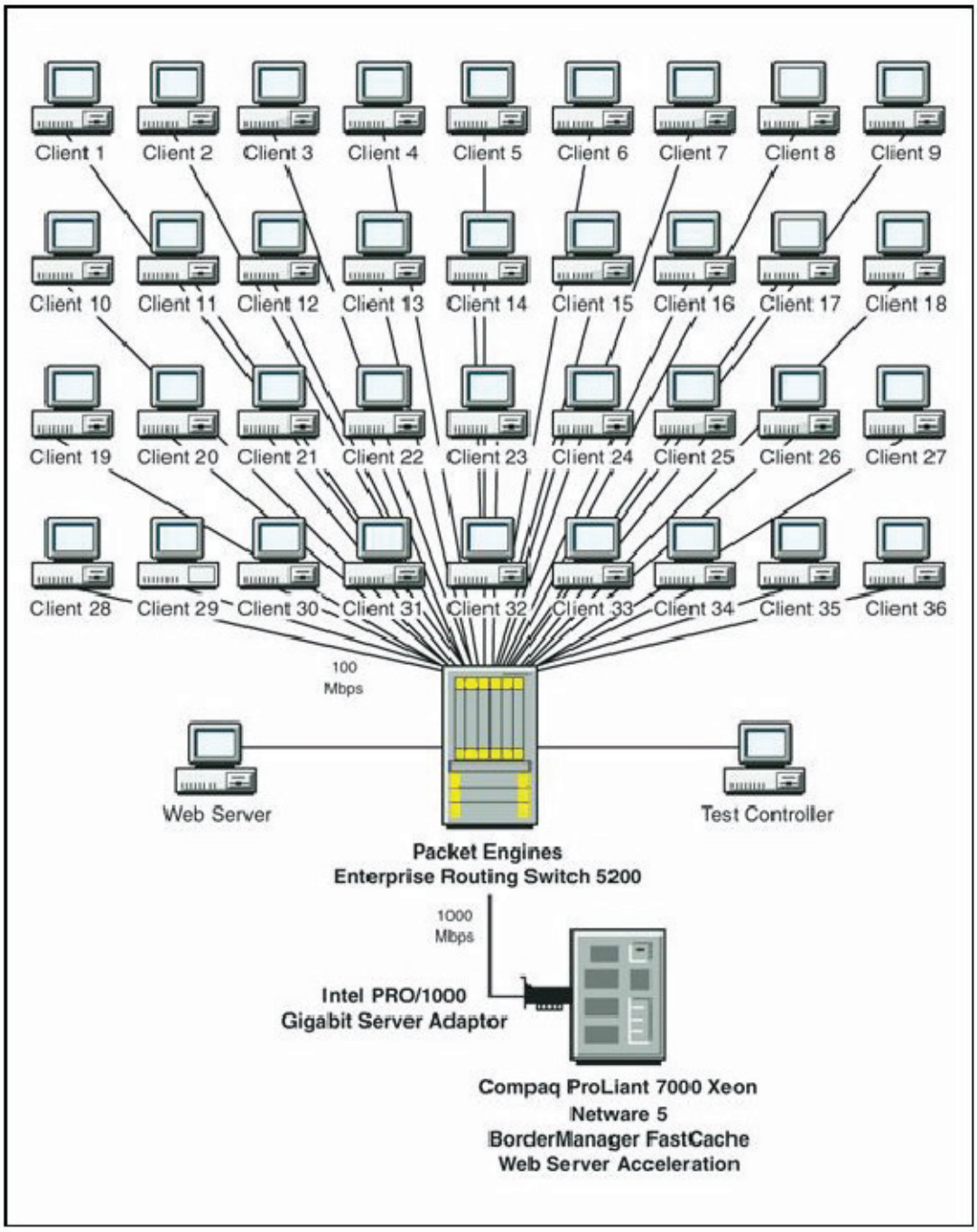
Αυτός ο τύπος απο Proxy Server χρησιμοποιεί επίσης την ιδέα του caching όπως ο κανονικός server αλλά είναι ρυθμισμένος με τέτοιο τρόπο που ο χρήστης δεν είναι χρειάζεται να κάνει ρυθμίσεις τον browser του. Σε γενικές γραμμές αυτού του τύπου οι proxy servers βασίζονται στο gateway και παρακολουθούν τις αιτήσεις απο τους χρήστες στο www (θύρα 80, 443, κτλ) φέρνουν το περιεχόμενο για μια φορά και σταδιακά απαντάνε στις αιτήσεις απο την μνήμη cache. Το όνομά τους βασίζεται στο γεγονός οτι δεν χρειάζεται καμία ρύθμιση στον χρήστη άρα κατά κάποιον τρόπο είναι transparent για τον χρήστη. Τέλος, χρησιμοποιούνται κυρίως για εταιρείες και μεγάλους οργανισμούς όπου είναι πάρα πολλοί οι χρήστες και είναι πολύ δύσκολο να ρυθμιστούν όλοι. Επιπλέον, χρησιμοποιούνται τους ISP's (ΟΤΕ κτλ) για να μειώσουν το φόρτο της γραμμής.

Reverse Proxy



Στην τελευταία κατηγορία έχουμε τον reverse proxy. Είναι τελείως διαφορετικός απο τους δυο παραπάνω κυρίως γιατί βοηθά τον ήδη υπάρχοντα web server και όχι τον χρήστη! Σε γενικές γραμμές αυτός είναι ο server που θα απαντήσει σε αιτήσεις που πηγαίνουν στον web server μόνο και μόνο για να μειώσει τον φόρτο των συνολικών συνδέσεων και αιτήσεων στον web server.Η παραπάνω ιδέα λέγεται και Web Server

Acceleration.



8.6 ΕΡΓΑΛΕΙΑ TOR

8.6.1 PRIVOXY

Ο οποιοσδήποτε που επιθυμεί ασφάλεια, ιδιωτικότητα και έλεγχο στην περιήγησή στο διαδίκτυο, μπορεί να χρησιμοποιεί το Privoxy. Τοσυγκεκριμένο πρόγραμμα ειδικά, είναι μια καλή επιλογή για αυτούς που χρειάζονται περισσότερη ασφάλεια. Το

Privoxy στηρίζεται πάνω στον web proxy server και χρησιμοποιείται σε συνδυασμό με το Tor. Και τα δύο μαζί δουλεύουν για να κρύψουν την ip διεύθυνση του υπολογιστή μας. Αυτό το καταφέρνουν με το να στέλνουν το σήμα μας σε ειδικούς servers του διαδικτύου, οι οποίοι αποκαλούνται onion routers.

Το Privoxy είναι ένας web proxy για HTTP συνδέσεις που μας δίνει πολλές δυνατότητες για προσαρμογές στα μέτρα μας και λειτουργικότητα.Με τη χρήση του Privoxy θα μπορούμε να διαχειριστούμε τα HTTP cookies, να φιλτράρουμε το περιεχόμενο και διαφημίσεις στο διαδίκτυο κ.ά. Το Privoxy έχει το πλεονέκτημα ότι όλα τα υπάρχοντα αιτήματα HTTP μπορούν να προωθηθούν. Αυτό είναι το αδύναμο σημείο του Tor. Το Tor μπορεί μόνο να προωθήσει κίνηση, αλλά όλα τα αιτήματα DNS (που αντιστοιχούν το όνομα του διακομιστή στην IP του server) προσπερνιούνται. Αυτό σημαίνει ότι η ανωνυμία δεν είναι πια εγγυημένη, καθώς κάποιος θα μπορεί να αναγνωρίσει την πραγματική IP στα αρχεία καταγραφής του server.

Για παράδειγμα όπως γίνεται με τις ταινίες κατασκόπων του Hollywood, οι οποίες δείχνουν ένα τηλεφώνημα που εντοπίζεται σε δεκάδες λάθοςπεριοχές.Έτσι γίνεται και με την IP μας όταν κρύβεται πίσω από αυτούς τους ειδικούς servers. Η πραγματική μας IP διεύθυνση όντως «εξαφανίζεται» όταν σερφάρουμε στο διαδίκτυο, ή στέλνουμε ένα e-mail ή «κατεβάζουμε» κάποια αρχεία μέσω του δικτύου Tor onion. Ο web proxy είναι μια υπηρεσία η οποία είναι φτιαγμένη με το ίδιο λογισμικό όπως το Privoxy, δηλαδή, οι clients μπορούν να συνδέονται απευθείας με τους servers διαδικτύου (web servers ή proxy servers).

Χαρακτηριστικά Privoxy:

- Μπορεί να κρατά ενεργές τις εξερχόμενες συνδέσεις και να τις επαναχρησιμοποιήσει αργότερα.
- Υποστηρίζει την αλλαγή συμπεριφοράς η οποία αφορά τις επικεφαλίδες των client και servers.
- Μπορεί να «τρέχει» ως ενδιάμεσος proxy server, ο οποίος προλαμβάνει την ανάγκη να χωριστούν οι μηχανές αναζήτησης χωριστά.
- Περιέχει περίπλοκες ενέργειες και φίλτρα για να χειρίζεται τις επικεφαλίδες των server και client.
- Μπορεί να φιλτράρει τις ιστοσελίδες, δηλαδή κάνει αντικατάσταση κειμένου, αφαιρεί τα bunner, διαθέτει ορατά εργαλεία για διαχείριση, αγνοεί τα επανεμφανιζόμενα παράθυρα και τα κομμάτια κώδικα javascript και html κλπ.
- Βελτιώνει τη διαχείριση των cookies.
- Υποστηρίζει πολυμέσα.
- Μπορεί να συνεργαστεί και με άλλους proxy servers.

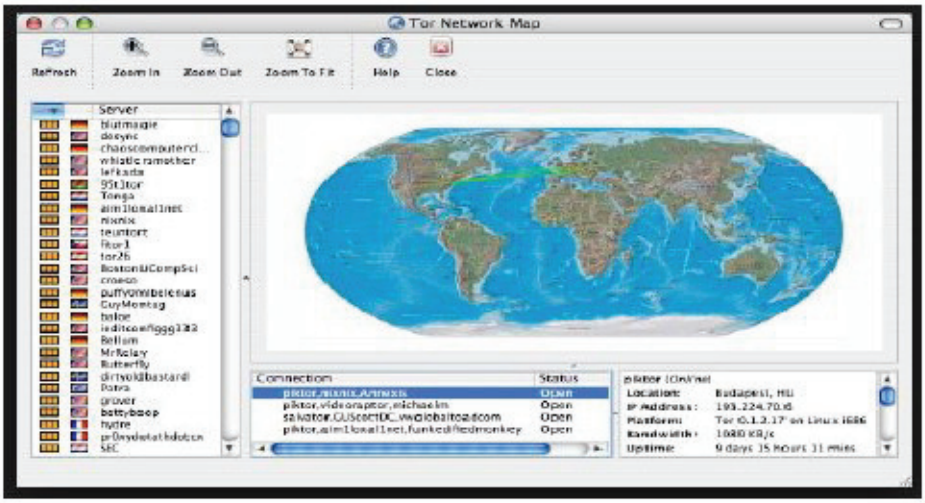
8.6.2 Vidalia

Το Vidalia είναι ένα πακέτο εφαρμογής το οποίο περιλαμβάνει το Tor, τον Privoxy

proxy, όπως επίσης και το Vidalia GUI (Graphical User Interface) για διαχείριση του Tor. Με τηνεγκατάσταση του Vidalia κατευθείαν φορτώνεται στον υπολογιστή μας ένας Privoxy proxy ο οποίος επιτυγχάνει τη σύνδεσή μας με το Tor δίκτυο. ToVidalia στην ουσία αναλαμβάνει τηνεγκατάσταση του Tor και του privoxy και τον εύκολο χειρισμό τους.

Vidalia control panel

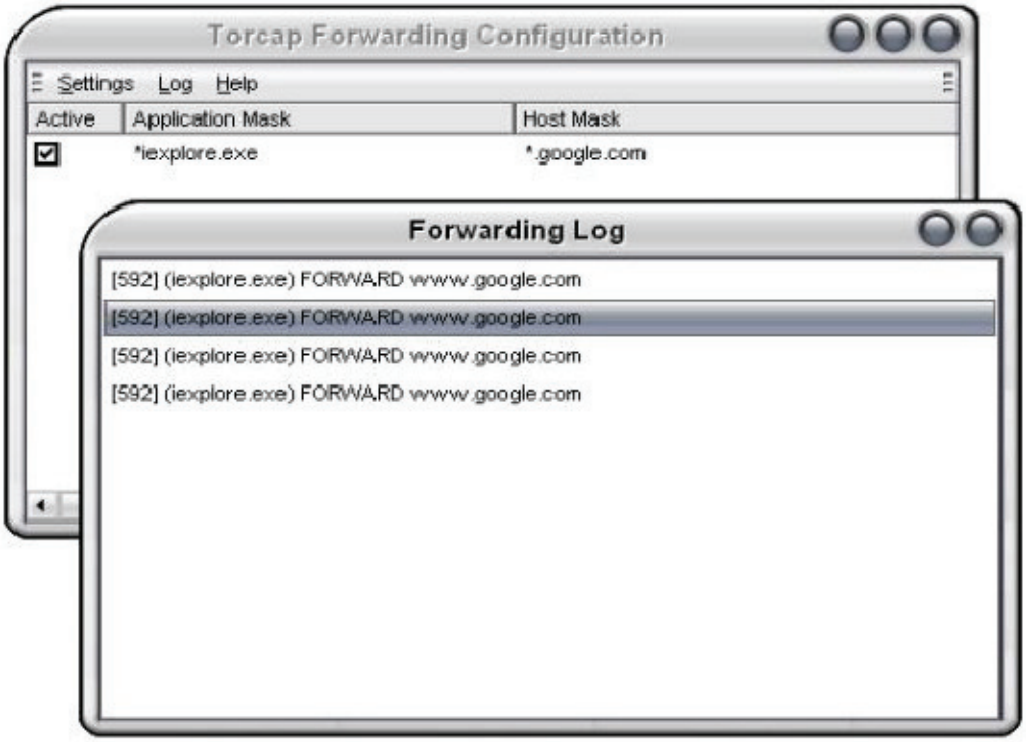
Οπίνακας ελέγχου του Vidalia μας δείχνει τη θέση σύνδεσής μας με το Tor και μας αφήνει να ξεκινάμε και να σταματά με τη σύνδεση, όπως επίσης και να αλλάζουμε τους proxies με τη χρήση ενός κατάλληλου κουμπιού το οποίο καλείται New Identity button. Το Vidalia επιπλέον προσφέρει μια γραφική αναπαράστασηστου bandwidth, έτσι ώστε να μπορούμε να δούμε πόση κίνηση έχουμε στείλει μέσω του Tor.



Vidalia Tor network map

8.6.3 Torcap

Το Torcap είναι ένα εργαλείο το οποίο επιτρέπει οποιαδήποτε δικτυακή εφαρμογή να συνδεθεί μέσωτου Tor, ακόμα και αν αυτή η εφαρμογή δεν υποστηρίζει τα socks.Λειτουργεί με το να εισάγει ένα DLL (Dynamic Link Library) σε κάθε διαδικασία πουτρέχει στον υπολογιστή του χρήστη. Αυτότο DLL δουλεύει με το Winsock API (Winsock Application Programming Interface) το οποίο συνεργάζεται τη παροχή DNS (Domain Name System) και τις συνδέσεις TCP/IP. Ηαπόφαση για το πότε θα συνδέεται ο χρήστης μέσωτ ου Tor ή απευθείας στο internet, εξαρτάται από την μάσκα της εφαρμογής (application mask) και τη μάσκα του εξυπηρετητή (host mask). Όταν αυτά τα δύο ταιριάξουν τότε η σύνδεση θα γίνει μέσω του Tor Socks server.



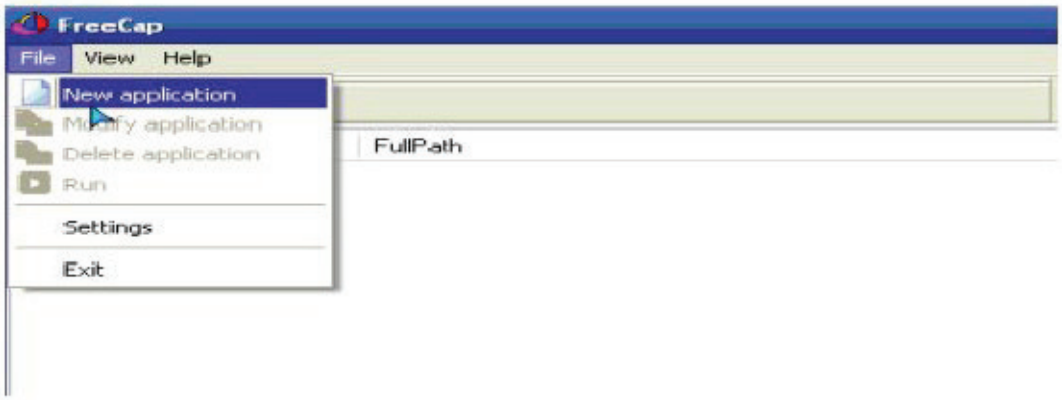
Torcap Forwarding Configuration

8.6.4 Torcap2

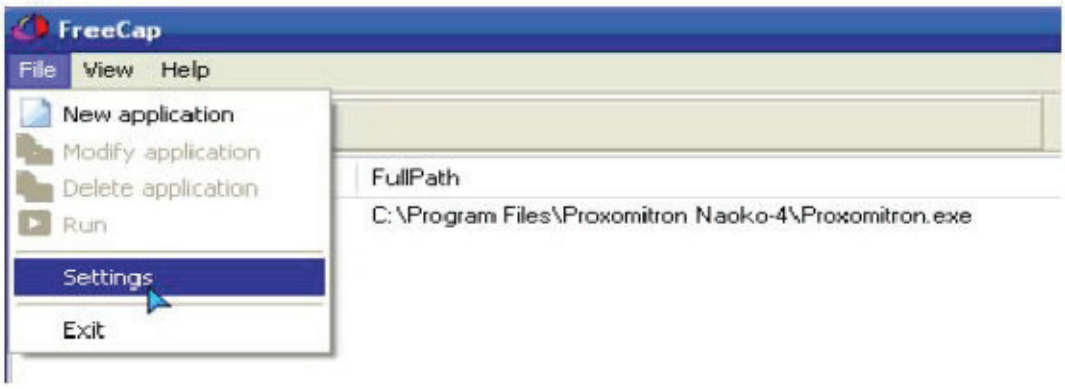
Το Torcap2 είναι ένα μικρό πρόγραμμα το οποίο βασίζεται πάνω στο Torcap και κάνει την ίδια λειτουργία, δηλαδή προσθέτει τα socks4a σε κάθε εφαρμογή που έχει πρόσβαση στο internet.Η διαφορά των Torcap και Torcap2 είναι ότι, το Torcap είναι γραμμένο σε Delphi και έχειμέγεθος περίπου 200K, ενώ το Torcap2 είναι γραμμένο σε C και το μέγεθός του είναι 50K.

8.6.5 Freecap

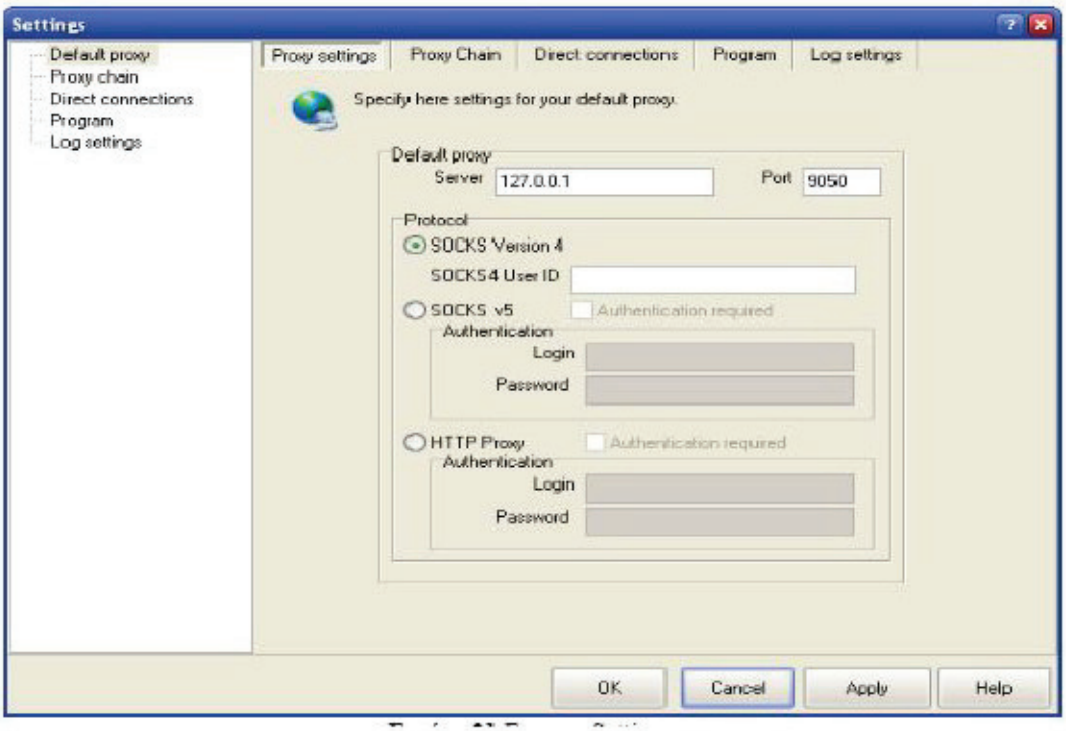
Το Freecap είναι ένα πρόγραμμα το οποίο ασχολείται με τις απευθείας συνδέσεις μέσω των socks servers.Αν κάποια προγράμματα δεν υποστηρίζουν τα socks πχ, ointernet explorer, τότε το Freecap είναι πολύ χρήσιμο σε αυτές τις περιπτώσεις γιατί αυτόματα περνάει όλες τις συνδέσεις μέσωτου socks server.



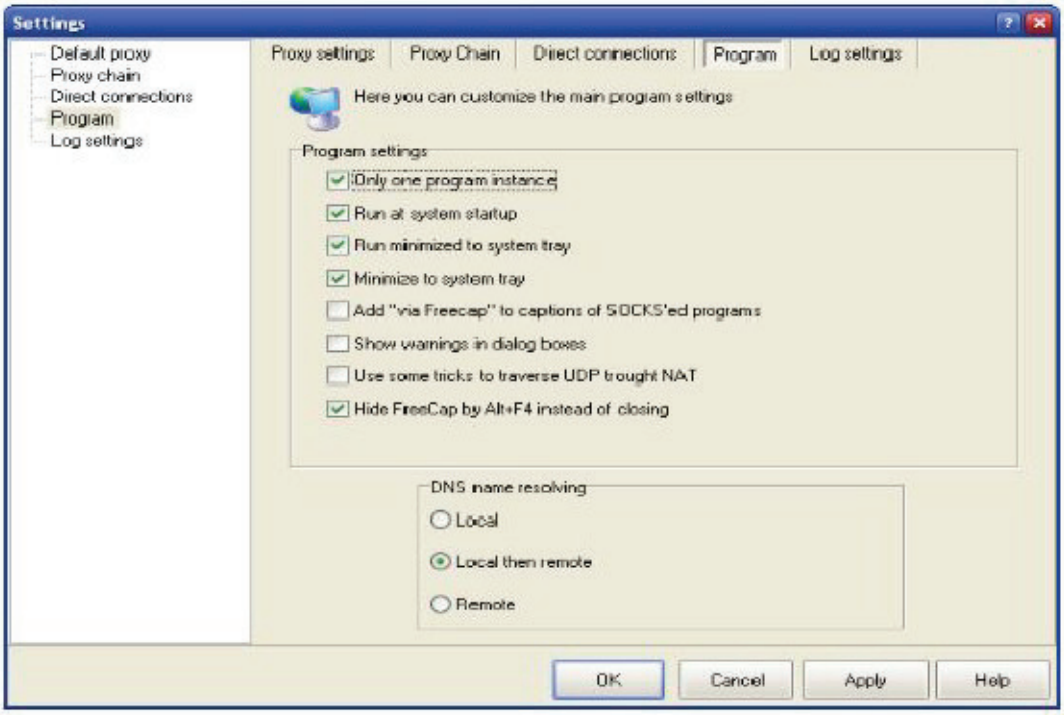
Freecap New Application



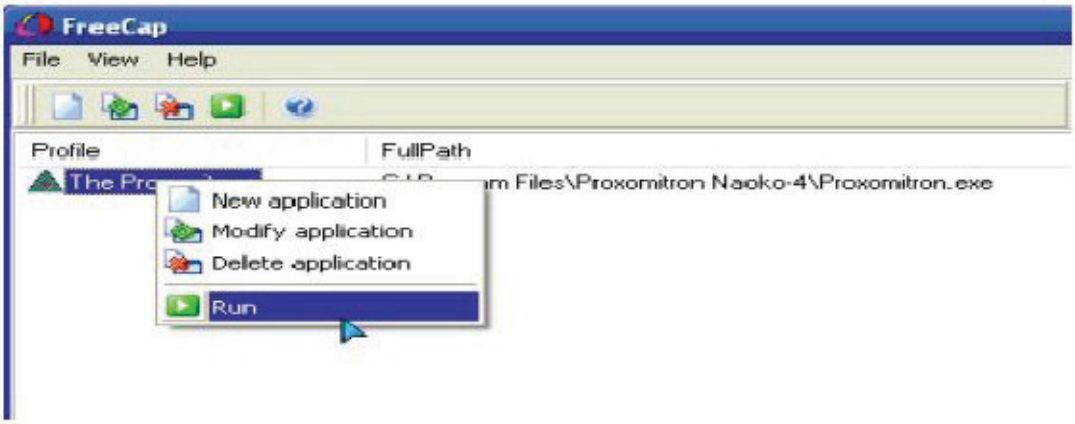
Freecap Settings



Freecap Settings



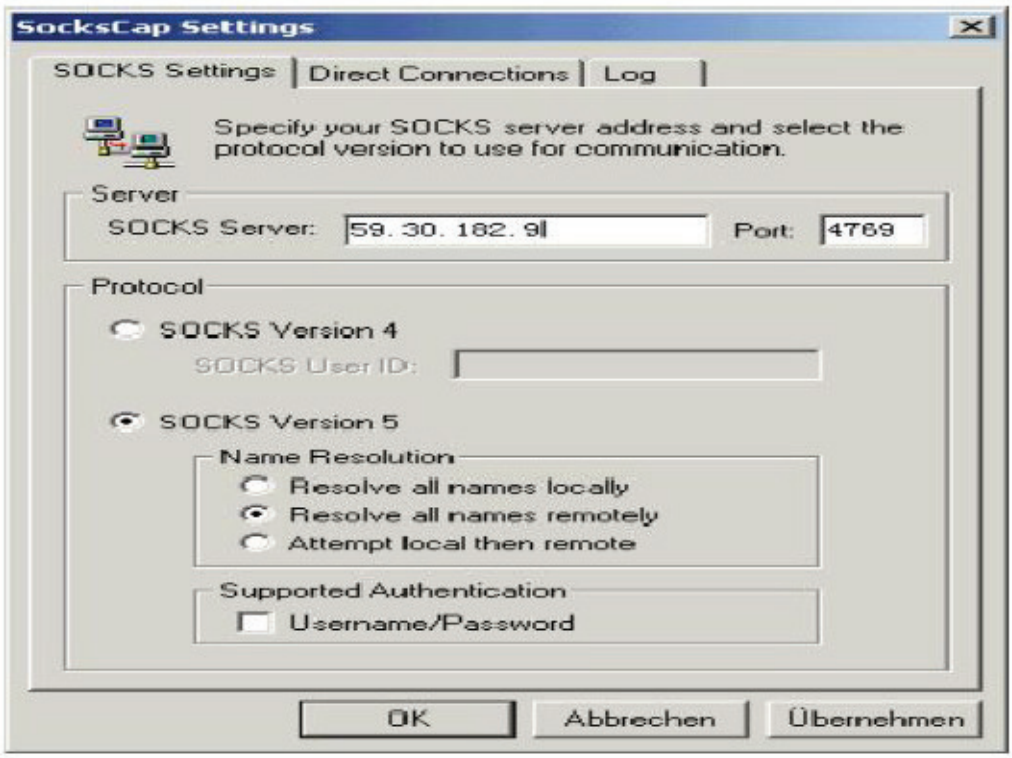
Freecap Settings



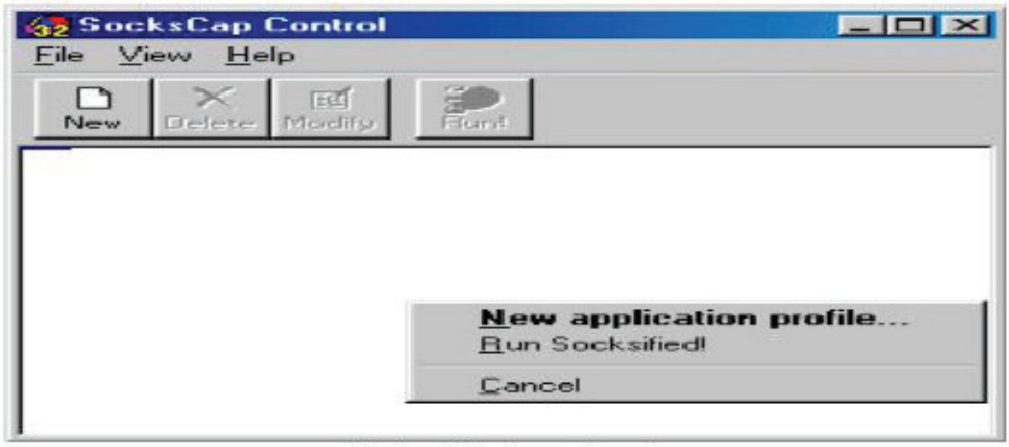
Freecap Run

8.6.6 Sockscap

Το Sockscap είναι ένα πρόγραμμα το οποίο λειτουργεί μέσω ενός socks server έκδοσης 4 ή 5, με αποτέλεσμα ο server που βρίσκεται στην άκρη της σύνδεσης να μην μπορεί να γνωρίζει τηναληθινή μας IP.

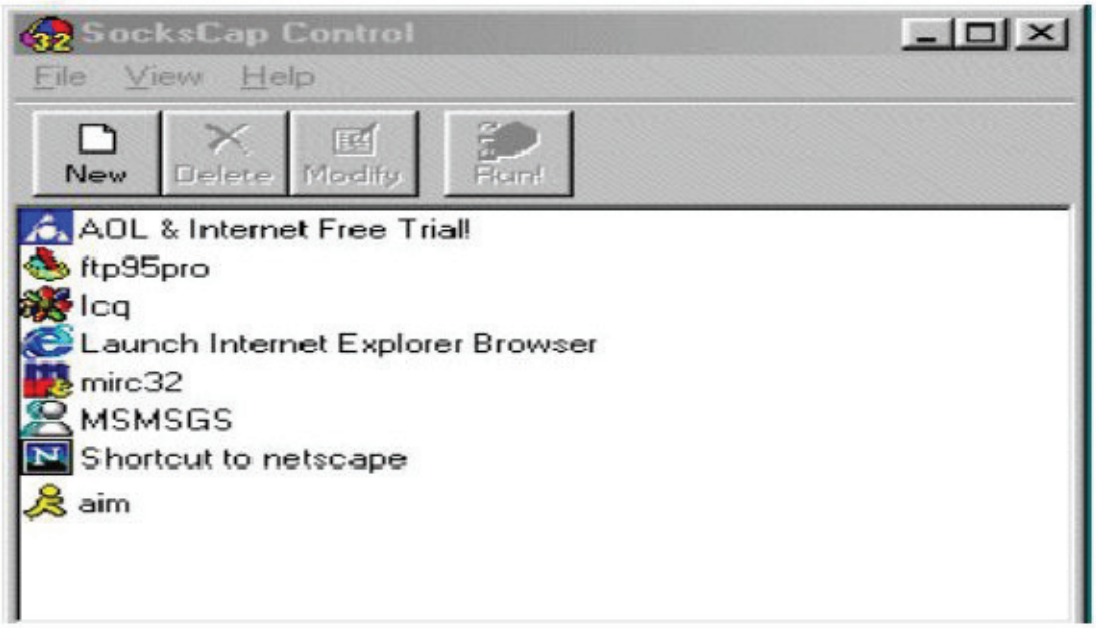


Sockscap Setting



Sockscap Control

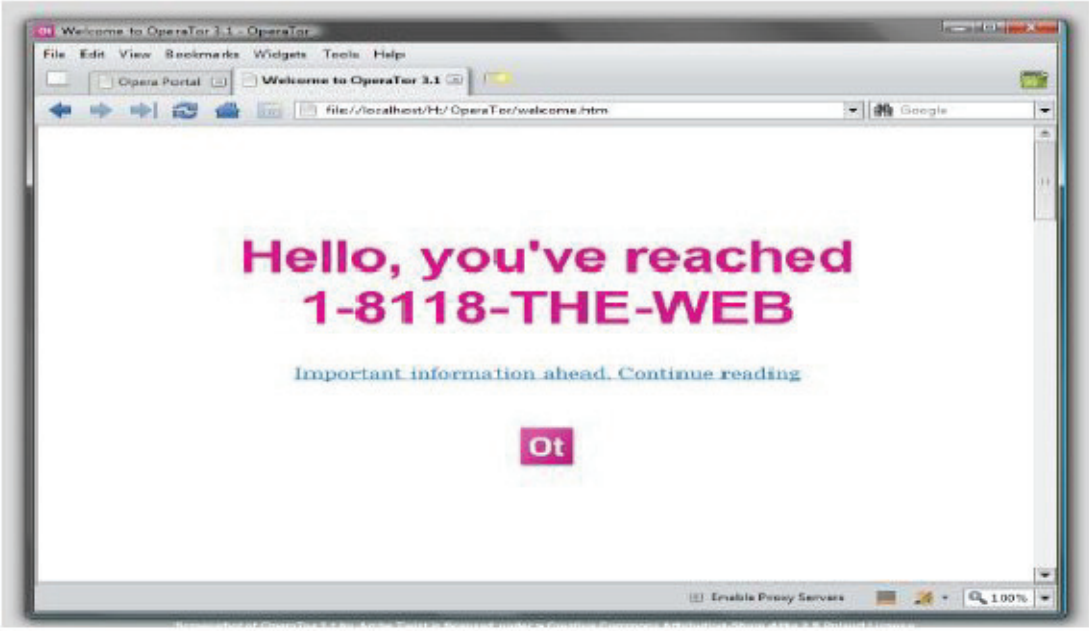
New Application Proflile



Sockscap Control

8.6.7 OperaTor

Το OperaTor είναι ένα πακέτο που μπορεί εύκολα να εγκατασταθεί σε κάποια φορητή μνήμη (usb stick, pendrive, εξωτερικόσκληρό) και επιτρέπει ανώνυμο σερφάρισμα σε δημόσιους χώρους (net cafes, δημόσιεςβιβλιοθήκεςκοκ) και όχι μόνο.Συνδυάζει τη δύναμη του Opera , του The Onion Router και του Privoxy. Με το OperaTor δεν θα αποθηκευτούν καθόλου πληροφορίες στο computer που έχουμε συνδέσει τη φορητή μνήμη. Μια σημαντική σημείωση είναι ότι οι ακόλουθες λειτουργίες δεν περνάνε ανώνυμες καθώς δεν χρησιμοποιούν τις proxy ρυθμίσεις τουOpera : Java, ενσωματωμένος διακομιστής Bittorrent, ενσωματωμένος διακομιστής e-mail και IRC.



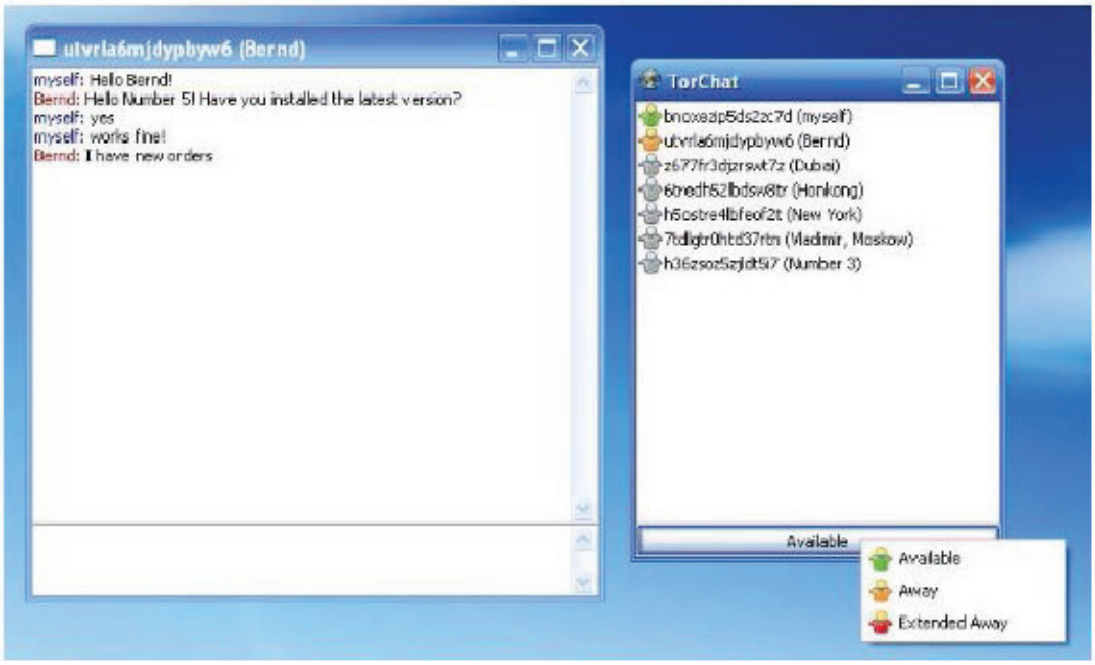
OperaTor

8.6.8 Xerobank browser

Το λογισμικό XeroBank μας δίνει τη δυνατότητα να «σερφάρουμε» ανώνυμα στο διαδίκτυο. Το XeroBank installer περιλαμβάνει το xB Browser, το xB Mail και το xB VPN.86O xB Browser χρησιμοποιείται για πρόσβαση στον web browser μέσω φορητής μνήμης και μπορεί να προσφέρει υψηλού επιπέδου ανωνυμία. Επίσης ο xB Browser κρυπτογραφεί τις δραστηριότητές μας και αποτρέπει τον εντοπισμό μας από κακόβουλους. Το xB Mail περιλαμβάνεται για τους Xerobank χρήστες, και χρησιμοποιείται για την πρόσβαση σεκ ρυπτογραφημένο e-mail. Το xB VPN χρησιμοποιείται για να δημιουργήσει μια VPN σύνδεση στο δίκτυο ανωνυμίας XeroBank. Έχεισχεδιαστεί για συνδέσεις OpenVPN και μπορεί να λειτουργήσει σε Windows 2k, NT, XP και Vista x64.

8.6.9 Tor Chat

Το TorChat είναι ένας peer to peer instant messenger και έχει σχεδιαστεί με βάση τις κρυμμένες υπηρεσίες του Tor.Μας παρέχει ισχυρή ανωνυμία και είναι πολύ εύκολο στη χρήσητου. Λειτουργεί μέσω ενός USB οδηγού σε οποιοδήποτε υπολογιστή που έχει λειτουργικό σύστηματα windows.



Using TorChat

ΚΕΦΑΛΑΙΟ 9

ΤΡΟΠΟΙ ΠΕΡΙΟΡΙΣΜΟΥ ΤΗΣ ΧΡΗΣΗΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ.

ΕΙΣΑΓΩΓΗ

Είναι κοινή πια παραδοχή πως όσο περνάει ο καιρός και αυξάνονται οι χρήστες του δικτύου, τόσο περισσότερο πλησιάζει το Internet την διάρθρωση και λειτουργία μιας πραγματικής κοινωνίας με δική της γλώσσα, συνήθειες, κώδικα συμπεριφοράς και ηθικής. Όπως όμως συμβαίνει σε κάθε κοινωνία, μερικά μέλη της, δεν ενστερνίζονται τις ηθικές αρχές του συνόλου, αλλά προτιμούν να λειτουργούν σε βάρος των πολλών αποκομίζοντας οικονομικά κυρίως οφέλη. Βέβαια, ακόμη και οι απατεώνες του δικτύου δεν μπορούν να ξεφύγουν από τους περιορισμούς που αυτό επιβάλλει. Οι τρόποι που χρησιμοποιούνται μέσα στο δίκτυο είναι πιο εγκεφαλικοί. Δεν είναι όμως λιγότεροεπικίνδυνοι.
Η απώλεια ψηφιακών δεδομένων αποτελεί μια από τις μεγαλύτερες μη υπολογιζόμενες ζημιές για μια σύγχρονη κοινωνία. Η προστασία δεδομένων από εξωτερικούς ή και εσωτερικούς κινδύνους όπως επίσης και η διασφάλιση της ομαλής λειτουργίας των υπολογιστικών συστημάτων ενός οικιακού ή εταιρικού δικτύου πρέπει να συγκαταλέγονται μεταξύ των προτεραιοτήτων όλων. Η μόλυνση ενός ή και περισσοτέρων συστημάτων από ψηφιακό ιό πολύ συχνά έχει ως αποτέλεσμα την καταστροφή ζωτικών δεδομένων για ένα πρόσωπο ή μια εταιρεία. Ένας hacker μπορεί να χρησιμοποιήσει εταιρικά ή προσωπικά δεδομένα με τρόπο ιδιαίτερα επιβλαβή για την ίδια την εταιρία ή το άτομο, χρησιμοποιώντας τα για οποιοδήποτε λόγο αυτός επιθυμεί. Παρακάτω παρουσιάζονται χρήσιμοι τρόποι και οδηγίες που μπορεί ένας χρήστης να ακολουθήσει ώστε να προφυλαχθεί από όλες τις απειλές που εγκυμονεί το Διαδίκτυο και επίσης προβάλλονται στατιστικά στοιχεία από τη χρήση του διαδικτύου τόσο από ενηλίκους όσο και από ανηλίκους.

9.1 Τάσεις επιθέσεων στο Internet.

Η εταιρεία Counterpane Internet Security, Inc. παρακολουθεί περισσότερα από 450 δίκτυα σε 35 χώρες σε κάθε χρονική ζώνη. Το 2004 παρακολούθησε 523 δισεκατομμύρια δικτυακά περιστατικά και οι αναλυτές της εξέτασαν 648,000 περιπτώσεις ασφαλείας. Παρακάτω ακολουθεί μία επισκόπηση της σημερινής κατάστασης στο Διαδίκτυο και οι εκτιμήσεις τους για τους επερχόμενους μήνες.

Το 2004, το 41% των επιθέσεων που εντόπισαν, επρόκειτο για μη εξουσιοδοτημένες δραστηριότητες κάποιου είδους, το 21% επρόκειτο για σαρώσεις, το 26% ήταν μη εξουσιοδοτημένη πρόσβαση, το 9% ήταν επιθέσεις άρνησης παροχής υπηρεσιών (DoS) και το 3% ήταν παράνομες χρήσεις εφαρμογών. Τους τελευταίους μήνες, οι δύο φορείς επιθέσεων που είδαν κατά συρροή ήταν κατά του Windows DCOM (Distributed Component Object Model), μέρος της υπηρεσίας RPC (απομακρυσμένη κλήση διαδικασίας) και της υπηρεσίας Windows LSASS.(υπηρεσία υποσυστήματος τοπικής ασφάλειας). Αυτές φαίνεται να ήταν οι τρέχουσες τάσεις για τους δημιουργούς ιών και σκουληκιών και η εκτίμηση τους ήταν ότι η τάση αυτή θα έχει και συνέχεια. Τους τελευταίους έξι μήνες του 2004, εντόπισαν μία πληθώρα επιθέσεων βασισμένων στις αδυναμίες φυλλομετρητών (όπως την αδυναμία εικόνων GDI-JPEG και IFRAME) και μία αύξηση σε επιθέσεις ευφυών σκουληκιών και ιών. Περισσότερα από 1,000 νέα σκουλήκια και ιοί ανακαλύφθηκαν τους τελευταίους έξι μήνες.
Το 2005, διέκριναν την κυκλοφορία ακόμη πιο σύνθετων σκουληκιών και ιών από ποτέ, ενσωματώνοντας σύνθετη συμπεριφορά: πολυμορφικά σκουλήκια, μεταμορφικά σκουλήκια και σκουλήκια που αποκρύπτουν το σημείο εισόδου. Για παράδειγμα, το SpyBot.KEG είναι ένα αναπτυγμένο σκουλήκι αξιολόγησης αδυναμιών που αναφέρει τις ανακαλυφθέντες αδυναμίες στο δημιουργό μέσω καναλιών IRC. Επίσης είδαν περισσότερες συνεπτυγμένες απειλές: κώδικας εκμετάλλευσης που συνδυάζει κακόβουλο κώδικα με αδυναμίες προκειμένου να πυροδοτήσει μια επίθεση. Ο διακομιστής IIS της Microsoft συνέχισε να αποτελεί έναν ελκυστικό στόχο. Αν και περισσότερες εταιρείες κινήθηκαν προς τα Windows 2003 και IIS 6, ωστόσο περίμεναν ότι οι επιθέσεις κατά του IIS θα μειωθούν. Τέλος, επισήμαναν τη χρήση ομότιμων δικτύων (peer-topeer) ως φορείς μετάδοσης ιών.
Μία άλλη τάση που διέκριναν είναι τα σκουλήκια με στοχοποίηση. Πρόσφατα, έχουν υπάρξει σκουλήκια που χρησιμοποιούν τεχνικές συλλογής δεδομένων τρίτων προσώπων, όπως η μηχανή αναζήτησης Google, για προηγμένη αναγνώριση. Αυτό οδήγησε σε περισσότερο ευφυή μεθοδολογία διάδοσης. Αντί να πραγματοποιούν επιθέσεις διασποράς (scattershot), τα σκουλήκια αυτά έχουν συγκεκριμένους στόχους. Αναγνωρίζοντας τους στόχους μέσω της συλλογής πληροφοριών τρίτων προσώπων, τα σκουλήκια έτσι μειώνουν το θόρυβο που θα έκαναν κανονικά όταν θα επέλεγαν στόχους στα τυφλά, με αποτέλεσμα να αυξάνουν το περιθώριο μεταξύ της απελευθέρωσης και του πρώτου εντοπισμού τους.
Ακόμη μία τάση του 2004 που ανέμεναν να αυξηθεί το 2005 είναι το έγκλημα. Το χάκινγκ έχει μεταφερθεί από χόμπι με στόχο την απόκτηση φήμης σε εγκληματική επιδίωξη με στόχο τα λεφτά. Οι χάκερς μπορούν να πουλήσουν άγνωστες αδυναμίες – «εργαλεία εκμετάλλευσης αδυναμιών ημέρας μηδέν» – στη μαύρη αγορά σε εγκληματίες που τις χρησιμοποιούν για να παραβιάσουν υπολογιστές. Οι χάκερς με δίκτυα παραβιασμένων μηχανημάτων μπορούν να βγάλουν λεφτά πουλώντας τα σε spammers ή ψαράδες (phisers). Μπορούν να τα χρησιμοποιήσουν για να επιτεθούν σε δίκτυα.. Ήδη υπάρχουν εγκληματικές πράξεις εκβιασμού από το Διαδίκτυο: χάκερς με δίκτυα παραβιασμένων μηχανημάτων απειλούν ότι θα πυροδοτήσουν επιθέσεις DoS κατά εταιρειών. Οι περισσότερες επιθέσεις έχουν στόχο περιφερειακές βιομηχανίες –

τζόγος στο Διαδίκτυο, παιχνίδια στο Διαδίκτυο, πορνογραφία στο Διαδίκτυο – καθώς και εξωχώρια δίκτυα (δίκτυα offshore). Όσο πιο επιτυχημένοι είναι οι εκβιασμοί αυτοί, τόσο πιο ατίθασοι θα γίνουν οι εγκληματίες. Επίσης υπάρχουν περισσότερες επιθέσεις κατά χρηματο-οικονομικών οργανισμών, εφόσον οι εγκληματίες ψάχνουν για νέους τρόπους για να διαπράξουν απάτη. Και οι περισσότερες εκ των έσω επιθέσεις γίνονται με κίνητρο το κέρδος. Ήδη οι περισσότερες στοχοποιημένες επιθέσεις – σε αντίθεση με τις επιθέσεις ευκαιρίας – πηγάζουν μέσα από το δίκτυο του οργανισμού κατά του οποίου γίνεται η επίθεση. Τέλος υπήρξαν περισσότερες ενέργειες χάκινγκ με πολιτικά κίνητρα, είτε κατά χωρών, κατά εταιρειών σε «πολιτικές» βιομηχανίες (πετροχημικά, φαρμακευτικά, κλπ) ή κατά πολιτικών οργανισμών. Αν και η εκτίμηση ήταν ότι τρομοκρατικές επιθέσεις δεν θα λαμβάνουν χώρα μέσα από το Διαδίκτυο, ωστόσο, πραγματοποιήθηκαν περισσότερες ενοχλητικές επιθέσεις από χάκερς με πολιτικά κίνητρα. Το Διαδίκτυο ακόμη παραμένει ένας επικίνδυνος χώρος, αλλά μεμονωμένα άτομα ή εταιρείες δεν θα το εγκαταλείψουν. Οι οικονομικοί και κοινωνικοί λόγοι που εμπλέκονται στη χρήση του Διαδικτύου είναι ακόμα πολύ ακαταμάχητοι.

9.2 Απειλές στο Web και τρόποι αντιμετώπισής τους.

Απειλή	Τρόπος Συλλογής Πληροφοριών	Τρόπος Αντιμετώπισης
Διαδικτυακή επαφή / γνωριμία (π.χ. άτομο με το οποίο συνδιαλέγεστε σε ένα chat room)	Μέσα από την ανάλυση των πληροφοριών που εσείς του δίνετε κατά την διάρκεια της συνομιλίας σας	Μην γνωστοποιείτε προσωπικές σας πληροφορίες. Δεν υπάρχουν τεχνολογίες αντιμετώπισης.
Άτομα του οικογενειακού/ εταιρικού σας περιβάλλοντος	Μέσα από την φυσική πρόσβαση στον υπολογιστή σας	Χρησιμοποιήστε passwords, hardware locks προηγμένης τεχνολογίας και κρυπτογράφηση δεδομένων
ISPs και παροχείς πρόσβασης στο Internet	Καταγραφή όλης της αναπτυσσόμενης δικτυακής δραστηριότητας	Με κρυπτογράφηση επικοινωνιών και χρήση proxy chains
Εταιρικά web sites	Cookies, Logs πρόσβασης	Proxying, realying, Anonymizer.com., Freedom.com, Crowds,

Network Infrastructure (VBNS, The Internet Cabal)	**Αναλύοντας την αναπτυσσόμενη δικτυακή δραστηριότητα όλου του Internet**	**Mix nets, remailers, rewebber, freedom, crowds**
System crackers, Network Attackers	**Σπάσιμο μηχανημάτων/ Network flooding/**	**Με ενημέρωση και διόρθωση για όλες τις πιθανές τρύπες του συστήματός σας/ με χρήση remailers (Publius, Freenet,).**
Number Crunchers (NSA, εταιρείες)	**Με το αργό σπάσιμο της κρυπτογραφίας που χρησιμοποιείτε**	**Χρησιμοποιήστε πιο ισχυρή μέθοδο κρυπτογράφησης**
Κυβερνήσεις	**Με τον έλεγχο όλης της δραστηριότητας στην περιοχή τους**	**Χρησιμοποιήστε υπηρεσίες όπως το FreeNet και το Freehaven, και άλλους ελεύθερους φορείς (έξω από την δικαιοδοσία της χώρας)**

9.3 Ο δρόμος για την online ασφάλεια.

Η επίτευξη της σχετικής ασφάλειας σε όλες τις διαδικτυακές δραστηριότητές δεν είναι καθόλου δύσκολη υπόθεση. Το μόνο που απαιτείται είναι να τηρούν οι χρήστες με σχεδόν θρησκευτική ευλάβεια μια σειρά κανόνων, οι οποίοι θα τους απαλλάξουν και θα τους προστατεύουν από κάθε λογής κίνδυνο που μπορεί να συναντήσουν στο Παγκόσμιο Διαδίκτυο.

updates και συνεχής ενημέρωση.

Ανά τακτά χρονικά διαστήματα (όχι μεγαλύτερα του ενός μήνα) πρέπει να γίνεται ένας έλεγχος στο Διαδίκτυο ή σε άλλες πηγές ενημέρωσης για την ύπαρξη ή τη διάθεση patches τόσο για το λειτουργικό σύστημα όσο και για το software που χρησιμοποιεί ο χρήστης. Για την ενημέρωση των Windows (98 και μεταγενέστερα) με τα τελευταία security fixes, καλύτερα είναι να προτιμά την λειτουργία Windows Update - που θα τον γλιτώσει από το μπελά του ψαξίματος, με μόνο αντίτιμο ίσως μια επιπλέον ολιγόλεπτη καθυστέρηση στα κατεβάσματα των updates. Το Microsoft Critical Update Notification, μια υπηρεσία που προσφέρεται για download στα Windows 2000 και είναι ενσωματωμένη στα Windows XP, ενημερώνει ανά πάσα στιγμή για το πότε ζωτικά updates είναι διαθέσιμα, αυτοματοποιώντας ως ένα βαθμό, μάλιστα, την ενημέρωση του συστήματος (one click download). Για άλλα σημαντικά patches ασφαλείας από την Microsoft η πιο έγκυρη πηγή ενημέρωσης είναι το Microsoft TechNet .

και "προσεγμένη" χρήση των δικτυακών εφαρμογών.

Το πρώτο μέλημα θα πρέπει να είναι η σωστή ρύθμιση των δικτυακών εφαρμογών που χρησιμοποιεί ο κάθε χρήστης. Οι περισσότεροι Web browsers διαθέτουν μερικές δεκάδες ρυθμίσεων ασφαλείας που καθορίζουν σε αρκετά μεγάλο βαθμό ποια components, ποια Java applets ή άλλα κοινά πλέον στοιχεία των web sites μπορούν να "εκτελεστούν" από τον browser, ενώ επιτρέπουν πλέον και μια πιο έξυπνη και ασφαλή διαχείριση των cookies (επιτρέποντας την αποθήκευσή τους στο σύστημα ή τη χρήση τους από τρίτα web sites μόνο όταν αυτό δεν συνιστά κίνδυνο για τα προσωπικά δεδομένα). Μια καλή αρχή για την δοκιμή των ρυθμίσεων του browser είναι το online test Qualys's Free Browser Checkup το οποίο κατά πάσα πιθανότητα θα αποκαλύψει στο χρήστη μερικές από τις αδυναμίες του browser του. Οι χρήστες των Windows μπορούν να στραφούν επιπλέον στη χρήση του Microsoft Baseline Security Analyzer. Πρόκειται για ένα δωρεάν διαθέσιμο από το TechNet εργαλείο που ελέγχει το σύστημά του για κακές ρυθμίσεις . Τέλος, αν χρησιμοποιεί instant messengers (κατηγορία προγραμμάτων που αποτελεί έως ένα βαθμό "κερκόπορτα" στην ασφάλεια των υπολογιστικών συστημάτων), πρέπει να αποφεύγει να συνομιλεί με ξένους .
Στην πλειοψηφία τους δημοφιλείς εφαρμογές, όπως ο AIM, το ICQ, το Trillian, ο Yahoo! και ο MSN Messenger, οι instant messengers συνήθως αποκαλύπτουν την IP διεύθυνση του συστήματος του κάθε χρήστη, ακόμα και σε ορισμένες περιπτώσεις που ο χρήστης έχει ζητήσει την απόκρυψή της, επιτρέποντας συνδέσεις peer to peer (απευθείας σύνδεση δύο υπολογιστικών συστημάτων). Επιπλέον, χρησιμοποιούν αρκετά ports (συμπεριλαμβανομένου και του 80 - του port που χρησιμοποιούν οι Web Browsers) αποτελώντας έτσι μια δημοφιλή "τρύπα" ασφαλείας για τους hackers. Ενδεικτικό, άλλωστε, για του λόγου το αληθές είναι ο μεγάλος αριθμός exploits που υπάρχουν για τους πιο δημοφιλείς instant messaging clients.

Σοφή χρήση Antivirus και Firewalls.

Ο χρήστης θα πρέπει πάντα να κάνει την καλύτερη επιλογή ενός ή και περισσότερων πακέτων antivirus και να φροντίζει να το ενημερώνει σε τακτική βάση με virus definition updates. Ακόμα και η πιο αποτελεσματική μηχανή αντιμετώπισης ιών, εάν δεν ενημερώνεται διαρκώς είναι τελείως άχρηστη. Στην πλειοψηφία τους, τα antivirus ελέγχουν όλα τα νέα αρχεία και τα νέαπρογράμματα που εγκαθίστανται στον υπολογιστή για ιούς, ωστόσο όπως και να 'χει θα πρέπει ο χρήστης να προγραμματίζει ένα εβδομαδιαίο πλήρη έλεγχο του συστήματος για κάθε ενδεχόμενο. Αναφορικά τώρα με τα firewalls, θα πρέπει να έχει κατά νου ότι οι εξ' ορισμού ρυθμίσεις των περισσοτέρων προγραμμάτων firewall θα επιτρέπουν απεριόριστη πρόσβαση στο Internet για μερικές χιλιάδες εφαρμογών. Δεν πρέπει να εμπιστευθεί με κλειστά μάτια σε αυτά την ασφάλεια του PC του. Αντιθέτως, πρέπει να ενεργοποιήσει τις μέγιστες ρυθμίσεις ασφαλείας και μέσα από μια συνεχή διαδικασία "δοκιμής και διαπίστωσης", να δώσει δικαιώματα χρήσης του Internet μόνο σε όσες εφαρμογές θέλετε ο χρήστης. Αρχικά θα πρέπει να αρνηθεί την χρήση/ πρόσβαση του Internet σε όλες τις

εφαρμογές (πλην του Web Browser/ e-mail client και οποιασδήποτε p2p file sharing εφαρμογής χρησιμοποιεί). Αν κάποια από αυτές δεν ανταποκρίνεται σωστά (στο σύνολο ή σε μέρος των λειτουργιών της) λόγω της μη πρόσβασης στο Internet, τότε πρέπει να δημιουργήσει ένα κανόνα εξαίρεσης στο πρόγραμμα firewall που χρησιμοποιεί .

Διατήρηση της ανωνυμίας.

Πρώτο βήμα στην διατήρηση της ανωνυμίας του χρήστη δεν είναι άλλο από την ενημέρωση του browser που χρησιμοποιεί. Αρχικά θα πρέπει να προτιμά την πιο πρόσφατη έκδοση (για τον Internet Explorer αυτήν την στιγμή η έκδοση 6.0) και φυσικά να φροντίζει να την ενημερώνει τακτικά με όλα τα security patches. Ο Internet Explorer 6 και ο Netscape 7 περιλαμβάνουν νέα χαρακτηριστικά που επιτρέπουν στο χρήστη ως ένα βαθμό να προστατέψει το απόρρητο των προσωπικών δεδομένων του και να διατηρεί την ανωνυμία του στο Διαδίκτυο. Τα νέα χαρακτηριστικά των browser εντοπίζονται κυρίως στην έξυπνη διαχείριση των cookies και στην αποτροπή εκτέλεσης "ύποπτου" κώδικα (malware). Στον Internet Explorer, για νααπενεργοποιηθούν τα third party cookies (τα cookies που "φυτεύονται" στο σύστημα όχι από τα sites που επισκέπτεστε αλλά από τριτογενείς φορείς), τότε ο χρήστης θα πρέπει να κάνει την ακόλουθη διαδικασία. Να επιλέξει Tools -> Internet Options και στην συνέχεια Privacy. Στη συνέχεια, να πάει στην ενότητα επιλογών Advanced και να ενεργοποιήσει την επιλογή "Override automatic Cookie Handling". Γενικότερα είναι προτιμότερο να επιτρέπονται τα πρωτογενή cookies, να μπλοκάρονται τα third party cookies και τέλος να επιτρέπονται τα session cookies (που συνήθως αφορούν σε μια περίοδο χρήσης/ επίσκεψης σε μια online υπηρεσία - webmail κτλ). Επόμενο βήμα στην προστασία της ανωνυμίας του δεν είναι άλλο από την χρήση ενός προγράμματος αποτροπής / παρεμπόδισης της λειτουργίας spyware λογισμικού

Κρυπτογράφηση και περιορισμός των υπηρεσιών.

Ο καθορισμός των υπηρεσιών (services) που θα είναι ενεργές σε ένα σύστημα με Windows XP (ή προγενέστερα NT based λειτουργικά συστήματα) είναι ίσως ένα από τα πιο κρίσιμα στάδια στην δημιουργία μιας ζώνης ασφαλείας για τον προσωπικό υπολογιστή ή το εταιρικό δίκτυο. Υπηρεσίες όπως Remote Registry, Remote Desktop , Remote Access μπορεί να είναι αρκετά χρήσιμα εργαλεία για διαχειριστές μεγάλων εταιρικών δικτύων. Ωστόσο είναι απίθανο το αν και πότε θα φανούν χρήσιμα σε ένα home user. Για να νιώθει περισσότερη ασφάλεια ο χρήστης, αλλά και για να μη βρεθεί προ εκπλήξεων αφού κάθε μια από αυτές δίνει σχεδόν απεριόριστη πρόσβαση στον υπολογιστή του, τότε αυτό που είναι απαραίτητο να κάνει είναι να τις απενεργοποιήσει. Επιπλέον, αν όντως τα δεδομένα που διατηρεί στο σκληρό δίσκο ή στο ηλεκτρονικό του ταχυδρομείο είναι τόσο "ευαίσθητα" και "προσωπικά" που δεν θέλει να τα δει κανείς άλλος, το κλείδωμα όλων των δικτυακών τρυπών στην ασφάλεια δεν είναι αρκετό. Για διάφορους λόγους, προτείνεται η χρήση

κρυπτογράφησης στα δεδομένα συγκεκριμένων φακέλων (π.χ. σε αυτούς που αποθηκεύει τα προσωπικά δεδομένα του), η οποία θα δυσκολέψει επιπρόσθετα το έργο των όποιων καλοθελητών. Για να κρυπτογραφήσει τα εμπεριεχόμενα αρχεία ενός καταλόγου στα Windows XP, μέσα από ένα παράθυρο του Windows Explorer, τότε πρέπει να επιλέξει τον κατάλογο και με δεξί κλικ Properties . Στην συνέχεια να πάει στην σελίδα General και κατόπιν να επιλέξει Advanced και ακολούθως "Encrypt".

Παρακολούθηση της δικτυακής δραστηριότητας.

Η παρακολούθηση και ο έλεγχος της εισερχόμενης/ εξερχόμενης δικτυακής κίνησης packets δεδομένων (outbound/ inbound traffic) μπορεί να αποκαλύψει στο χρήστη αρκετά πράγματα για την παρασκηνιακή δραστηριότητα εφαρμογών που υπό άλλες συνθήκες θα περνούσε απαρατήρητη. Πρόκειται ίσως για μια πιο μακρόχρονη διαδικασία εύρεσης και αντιμετώπισης trojan και spyware εφαρμογών που ωστόσο μπορεί να δώσει λύσεις εκεί που ένα ή anti spyware πρόγραμμα ενδεχομένως να αποτύχει. Πέρα από τη μη εγκεκριμένη εκροή packets από το σύστημα προς τον "έξω κόσμο" του Διαδικτύου, η παρακολούθηση της δικτυακής δραστηριότητας μπορεί να αποκαλύψει τον τρόπο δράσης κάποιων hackers, δίνοντας του εμμέσως πλην σαφώς κατευθυντήριες γραμμές για την περαιτέρω προάσπιση του συστήματός η του δικτύου του. Παρότι τα Windows XP διαθέτουν κάποιες απλοϊκές λειτουργίες επισκόπησης της δικτυακής δραστηριότητας, συνιστάται ανεπιφύλακτα η χρήση εξειδικευμένου εργαλείου .

9.4 Ανωνυμία στο διαδίκτυο. Τεχνικές και λύσεις διατήρησης της ανωνυμίας στο Διαδίκτυο

9.4.1 Proxy και Proxy Chains.

Η αρχαιότερη τεχνολογία και η βάση όλων των ανώνυμων επικοινωνιών στο Διαδίκτυο είναι ο proxy. Ο proxy είναι ένας υπολογιστής στο δίκτυο, ο οποίος αναλαμβάνει να προωθήσει ένα "μήνυμα" που αποστέλλει ένας υπολογιστής Α σε ένα υπολογιστή Β, φροντίζοντας έτσι ώστε να μην αποκαλυφθεί ποτέ η πηγή του μηνύματος. Ένας τέτοιος proxy, δηλαδή ένας proxy που κατορθώνει επιτυχώς να αποκρύψει την ταυτότητα του αποστολέα του μηνύματος καλείται "anonymizer".
Οι "anonymizer" προέκυψαν ως απομιμήσεις τις καθημερινής ζωής, π.χ. στην συχνή περίπτωση που ένας δημοσιογράφος μεταφέρει μια είδηση αρχίζοντας με την φράση "Σύμφωνα με πηγές" και άλλα τετριμμένα χωρίς ωστόσο να κατονομαστεί η πηγή του μηνύματος, τότε έχουμε να κάνουμε με ένα "anonymizer". Όταν ένα μήνυμα περνάει από μια αλυσίδα anonymizers, περνάει μέσα από ένα σύστημα υπολογιστών που καλείται proxy chains (αλυσίδα από proxies) Πιο αποτελεσματικοί proxy chains είναι αυτοί που υποστηρίζουν ισχυρή κρυπτογράφηση δεδομένων.

9.4.2 Mixnets και Mixnet Reply Blocks.

Τα Mixnets πρωτοεμφανίστηκαν το 1981 από τον David Chaum. Βασική έννοια στα Mixnets είναι ο MIX, ο οποίος είναι ένας proxy που αποδέχεται τα κρυπτογραφημένα μηνύματα με το Public key (μέθοδος πιστοποίησης ταυτότητας που λειτουργεί ως κλειδί για την αποκρυπτογράφηση της πληροφορίας), τα αποκωδικοποιεί, τα ταξινομεί και τα προωθεί στον τελικό τους αποδέκτη, διαγράφοντας όλες τις πληροφορίες για την πηγή τους. Επιπλέον, ο Chaum, καθόρισε τον τρόπο με το οποίο η χρήση αλυσίδων από Mix μπορεί να οδηγήσει στην τελική διαγραφή όλων των στοιχείων που αποδεικνύουν την ταυτότητα του αποστολέα. Ένα mixnet τώρα συνιστά ένα κόμβο υπολογιστών, καθένας από τους οποίους έχουν ένα ζεύγος public/secret keys. Το μήνυμα φθάνει κρυπτογραφημένο στο πρώτο MIX, αποκρυπτογραφείται, κρυπτογραφείται και στην συνέχεια περνάει στο επόμενο MIX όπου ακολουθείται πάλι η ίδια διαδικασία μέχρι ναφθάσει στον τελικό MIX και να ανακατευθυνθεί στον τελικό αποδέκτη. Όσο πιο μεγάλη είναι η αλυσίδα των MIX τόσο πιο δύσκολο είναι για κάποιον να εντοπίσει την πηγή του μηνύματος.
Η πολυπλοκότητα των MIXnets καθώς επίσης και η δεδομένη καθυστέρηση που παρατηρείται στην αποστολή του μηνύματος, τα καθιστούν μη πρακτικά για χρήσεις όπως Web browsing ή και συμμετοχή σε chat rooms και σε άλλα μέρη όπου υπάρχει απαίτηση για συνεχή διάδραση. Τα MIXnets Reply Blocks, καθορίζουν πέρα από την αποστολή του μηνύματος και τη διαδρομή της απάντησης σε αυτό, αναγκάζουν, δηλαδή, τον αποδέκτη του μηνύματος να απαντήσει χρησιμοποιώντας την ίδια ή παρεμφερή ασφαλή διαδικασία.

9.4.3 Remailers.

Τα προγράμματα που χρησιμοποιούνται για την ανωνυμία στο e-mail είναι ευρύτατα γνωστά ως remailers. Όπως σε όλες τις κατηγορίες των εργαλείων διατήρησης της ανωνυμίας (anonymity tools), τα remailers χρησιμοποιούν και τις δύο προαναφερόμενες τεχνολογίες (Proxy/ Mixnets) και διακρίνονται σε τρεις κατηγορίες:
τύπου 0: remailers που χρησιμοποιούν έναν μόνο proxy
τύπου 1: remailers που χρησιμοποιούν ένα mixnet
τύπου 2: remailers που χρησιμοποιούν mixnets με reply blocks

Τύπος Remailer: Ο:
Διατηρεί πίνακες με πλασματικές και πραγματικές e-mail διευθύνσεις. Υπάρχει μόνο ένα σημείο που "κλειδώνει" την επικοινωνία.
Τύπος Remailer: 1:
Χρησιμοποιούν τα δοσμένα public keys για να κρυπτογραφήσουν τα εισερχόμενα μηνύματα, ενώ παρέχουν anonymous e-mail μέσα από την χρήση των reply blocks.
Τύπος Remailer: 2:
Διακρίνονται από όλα τα χαρακτηριστικά των cypherpunks σε συνδυασμό με:
• το καθορισμένο σταθερό μέγεθος των μηνυμάτων
• την ανακατανομή τους

• τη μη σταθερή καθυστέρηση κατά την μεταφορά τους από hop σε hop

Καθένας από αυτούς τους τύπους απευθύνεται σε ξεχωριστό κοινό. Συγκεκριμένα, ο πρώτος απευθύνεται κυρίως σε αρχάριους χρήστες που επιθυμούν μία μέθοδο επικοινωνίας ασφαλέστερη εκείνης που προσφέρει ο mail server του ISP τους (ή οι παροχείς Web mail), ο δεύτερος σε κοινό με μεγαλύτερες απαιτήσεις σε θέματα ασφαλείας και ο τρίτος στους σκληροπυρηνικούς θιασώτες της ασφάλειας και της ανωνυμίας στο Internet.

9.4.4 Ανώνυμο Web surfing.

Μια σειρά από ολοκληρωμένες προτάσεις, που ξεφεύγουν από την δυνατότητα αποστολής ανώνυμου e-mail λύνουν τα χέρια σε όλους τους χρήστες δίνοντάς τους όλα τα απαραίτητα μέσα για ανώνυμο web surfing. Αυτές οι υπηρεσίες αναλαμβάνουν το σύνολο των λειτουργιών ενός proxy server, αποκρύπτοντας την IP διεύθυνση που χρησιμοποιείται και δεχόμενες τα cookies και μια σειρά άλλα δεδομένα για λογαριασμό τους. Οι σημαντικότερες υπηρεσίες αυτής της κατηγορίας είναι:

Anonymizer

Κατά πάσα πιθανότητα, το Anonymizer είναι το πιο γνωστό από όλες αυτές τις υπηρεσίες, αποτελώντας για πολλούς χρήστες την πρώτη γνωριμία με το "ανώνυμο Web". Η εταιρεία, ανάλογα με το κόστος συνδρομής, προσφέρει διάφορα πακέτα υπηρεσιών και δωρεάν χρήση της υπηρεσίας για Web surfing. Στο πλαίσιο της δωρεάν παρεχόμενης υπηρεσίας συμπληρώνει ο χρήστης μια απλή φόρμα στο site του Anonymizer, προκειμένου να επιτραπεί η εισαγωγή μιας Web διεύθυνσης (URL - Uniform Resource Locator) και η θέασή της μέσω του δικτύου του Anonymizer. Ωστόσο, αν κάνει κλικ μέσα στον browser παρακάμπτεται η χρήση του anonymizer (θα πρέπει να βλέπει διαδοχικά τις σελίδες μέσα από την φόρμα του anonymizer). Η συνδρομή στο βασικό πακέτο Anonymous Surfing τον απαλλάσσει από αυτό το πρόβλημα, ενώ για μερικά χρήματα παραπάνω το anonymizer προσφέρει και κρυπτογράφηση δεδομένων (με χρήση 128 bit κρυπτογράφησης SSL3). Το πλήρες πακέτο υπηρεσιών (dial up) , περιλαμβάνει IP masking, κρυπτογράφηση αλλά και αυξημένη ταχύτητα αφού αποκτά απευθείας πρόσβασης στο δίκτυο του Anomymizer. Από τα βασικότερα μειονεκτήματα του Anonymizer είναι η έλλειψη της υποστήριξης Java (γλώσσα προγραμματισμού ανεξάρτητη από πλατφόρμες, αρχιτεκτονικές και λειτουργικά συστήματα).

Freedom

Το Freedom φαντάζει και είναι πιο ελκυστικό από οικονομικής απόψεως από το Anonymizer, αφού το κόστος του δεν υπερβαίνει τα €50 ετησίως. Με αυτά τα λεφτά δίνει πρόσβαση στο χρήστη, στις υπηρεσίες του μεσαίου πακέτου του Anonymizer

(anonymous proxy, πρόσβαση στο Internet και κρυπτογράφηση δεδομένων), ενώ για την αξιοποίηση της υπηρεσίας απαιτείται η χρήση ειδικού προγράμματος clients. Το Freedom διαφοροποιείται σε σχέση με τοAnonymizer στη χρήση πολλαπλών nyms, δηλαδή στη χρήση εναλλακτικών προσωπικοτήτων κάθε μια από τις οποίες μπορεί να προσαρμόσει σε διαφορετικές ανάγκες. Για παράδειγμα, ένα nym που χρησιμοποιείται κυρίως για επιχειρηματικούς σκοπούς μπορεί να φανερώνει στοιχεία της επαγγελματικής του ιδιότητας, ενώ ένα άλλο που χρησιμοποιείται για. κοινωνικούς σκοπούς νααποκαλύπτει το φύλο του, χωρίς ωστόσο να είναι δυνατή σε οποιοδήποτε σημείο χρήσης της υπηρεσίας η διασταύρωση και η ταυτοποίηση αυτών των δύο nyms.

FreeNet

Το 1999 στο καταστατικό λειτουργίας της υπηρεσίας διαφαινόταν κάτι το πραγματικό επαναστατικό, δεδομένου ότι τότε το θέμα "ανωνυμία στο Διαδίκτυο" ήταν επίκαιρο όσο και σήμερα. Δυστυχώς, για διάφορους λόγους, η εξέλιξη του προγράμματος δεν ήταν η αναμενόμενη, ενώ ποτέ δεν έτυχε της δημοτικότητας που του άξιζε. Πλέον από κάτι που θα έφερνε τα πάνω - κάτω στο Διαδίκτυο, το FreeNet έχει εξελιχθεί σε μια άρτια υπηρεσία anonymous web surfing/file sharing, δημοφιλή κυρίως μεταξύ των κλειστών underground κοινοτήτων διακίνησης λογισμικού και mp3 αρχείων. Το FreeNet χαίρει της υποστήριξης της κοινότητας του open source, ενώ το επίπεδο των υπηρεσιών είναι πολύ καλύτερο από αυτό των συνδρομητικών υπηρεσιών, αφού ουσιαστικά έχουμε να κάνουμε με ένα δίκτυο μέσα στο δίκτυο.

9.4.5 Τεχνικές Προστασίας σε περιπτώσεις δημοσίευσης προσωπικών Δεδομένων.

Τηλεφωνικοί κατάλογοι του Διαδικτύου, υπηρεσίες αναζήτησης προσώπων και άλλοι κατάλογοι του Διαδικτύου καθιστούν σχεδόν αδύνατη τη διατήρηση των προσωπικών δεδομένων επικοινωνίας ενός χρήστη εκτός του Web. Είναι αρκετά εύκολο για τον οποιονδήποτε να βρει το όνομά, τον αριθμό τηλεφώνου, τη διεύθυνση οικίας ή τη διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη και να χρησιμοποιήσει τις πληροφορίες αυτές για επιχειρηματικούς ή κοινωνικούςσκοπούς, για διαφήμιση ή μάρκετινγκ ή ακόμη και με εγκληματική πρόθεση. Παρακάτω περιγράφουμε ορισμένους τρόπους που σκοπό έχουν να βοηθήσουν τον έλεγχο της ποσότητας των προσωπικών στοιχείων που δημοσιοποιεί ο οποιοσδήποτε χρήστης στον κόσμο, ενώ παράλληλα μπορεί να συνεχίσει να απολαμβάνει όλα τα οφέλη που του προσφέρει το Διαδίκτυο.

Προτού δημοσιεύσετε οποιαδήποτε πληροφορία στο Διαδίκτυο:

Να είστε εκλεκτικοί. Από την πρώτη κιόλας στιγμή, περιορίστε την ποσότητα των προσωπικών στοιχείων που δίνετε σε μια τοποθεσία. Αποκαλύψτε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας μόνον σε πρόσωπα που γνωρίζετε και αποφύγετε να

καταχωρείται οποιαδήποτε πληροφορία σε μεγάλους καταλόγους του Διαδικτύου.

Όταν κάνετε αγορές μέσω Διαδικτύου, θα πρέπει να γνωρίζετε τις πηγές από τις οποίες προμηθεύεστε προϊόντα. Οι προμηθευτές που πωλούν ηλεκτρονικές συσκευές με πολύ μεγάλη έκπτωση τείνουν να διαφέρουν από εκείνους που πωλούν, για παράδειγμα, είδη πλεξίματος. Όταν αγοράζετε ακριβά, δημοφιλή αντικείμενα, να τα αγοράζετε από διακεκριμένες εταιρείες πουδιαθέτουν σαφείς πολιτικές απορρήτου. Και μάθετε τι λένε οι άλλοι για τους πωλητές και τις διαδικτυακές τους τοποθεσίες, ανατρέχοντας σε παρατηρήσεις πωλητών και αγοραστών και ελέγχοντας διαδικτυακές τοποθεσίες σύγκρισης όπως, για παράδειγμα, το Epinions.com ή το Bizrate.com.

Διαβάστε προσεκτικά τη δήλωση για την προστασία των προσωπικών δεδομένων της εκάστοτε τοποθεσίας Web. Η δήλωση αυτή θα πρέπει να αναφέρει τον τρόπο με τον οποίο συλλέγονται τα προσωπικά σας στοιχεία από μια εταιρεία, καθώς και το σκοπό για τον οποίο συλλέγονται. Εάν κάτι δεν σας φαίνεται σωστό, επικοινωνήστε με την εταιρεία για να απαντήσουν στις ερωτήσεις σας, προτού αποκαλύψετε οποιαδήποτε προσωπικά στοιχεία. Εάν στην τοποθεσία δεν δημοσιοποιείται πολιτική προστασίας προσωπικών δεδομένων, τότε αναζητήστε άλλη τοποθεσία για να κάνετε τη δουλειά σας.

Δημοσιεύστε το βιογραφικό σας μόνο σε διακεκριμένες τοποθεσίες απασχόλησης. Βεβαιωθείτε ότι οι τοποθεσίες απασχόλησης που χρησιμοποιείτε διαθέτουν πολιτικές προστασίας προσωπικών δεδομένων οι οποίες επιτρέπουν την πρόσβαση στα προσωπικά σας στοιχεία μόνο από πιστοποιημένα γραφεία ευρέσεως εργασίας. Μην δημοσιοποιείτε το βιογραφικό σας στη δική σας τοποθεσία Web.

Βγείτε από τους καταλόγους (και μείνετε εκτός).

Μάθετε τις τοποθεσίες στις οποίες είστε καταχωρημένοι την τρέχουσα χρονική περίοδο, κάνοντας τη δική σας έρευνα στο Διαδίκτυο. Κάντε αναζήτηση του ονόματός σας στις δημοφιλείς μηχανές αναζήτησης αλλά και σε καταλόγους του Διαδικτύου όπως, για παράδειγμα, εκείνους που αναγράφονται στο πλευρικό κείμενο, στο δεξί μέρος της οθόνης σας.

Ζητήστε να διαγραφεί το όνομά σας από καταλόγους του Διαδικτύου. Εάν δεν είναι ξεκάθαρο το πώς μπορείτε να το κάνετε αυτό σε μια τοποθεσία Web, τότε χρησιμοποιήστε το σύνδεσμο "Contact Us" (Επικοινωνήστε μαζί μας) ή τη διεύθυνση στο κάτω μέρος της διαδικτυακής τοποθεσίας του καταλόγου.

Προμηθευτείτε έναν απόρρητο αριθμό τηλεφώνου ή τουλάχιστον φροντίστε ώστε να διαγραφούν οι καταχωρίσεις που αφορούν τη διεύθυνσή σας. Επίσης, δώστε εντολή στον πάροχο του τηλεφώνου σας και στον πάροχο των υπηρεσιών Διαδικτύου σας να αφαιρέσουν οποιαδήποτε προσωπικά σας στοιχεία από όλους τους καταλόγους τους.

Δημιουργήστε μια ειδική ηλεκτρονική διεύθυνση αποκλειστικά για τις δραστηριότητες στο Διαδίκτυο όπως, για παράδειγμα, για τις αγορές και τις ομάδες ενημέρωσης. Με αυτόν τον τρόπο, μπορείτε να την κλείσετε, εάν χρειάζεται, και να ανοίξετε μια νέα χωρίς να προκαλέσετε αναστάτωση στην εταιρεία σας ή στην προσωπική σας αλληλογραφία μέσω ηλεκτρονικού ταχυδρομείου.

Κρατήστε αρχείο, κάθε φορά που δίνετε τα προσωπικά σας στοιχεία σε μια εταιρεία, ούτως ώστε να μπορείτε να τους ζητήσετε να τα διαγράψουν αργότερα, εάν είναι απαραίτητο.

9.4.6 Μέτρα για την ασφάλεια του ηλεκτρονικού υπολογιστή.

Σημαντικό για την ασφάλεια του ηλεκτρονικού υπολογιστή είναι τα ειδικά προϊόντα ασφαλείας, που καλύπτουν τόσο σε επίπεδο hardware (ο «ορατός» εξοπλισμός ενός συστήματος)όσο και σε επίπεδο λογισμικού (software). Επίσης το επισφαλές ενός υπολογιστή καθορίζεται από το διάστημα που είναι συνδεδεμένος όπως επίσης και από την ταχύτητα της σύνδεσής του. Η χρήση firewalls, antivirus (αντιβιοτικών) προγραμμάτων και λογισμικού προστασίας προσωπικών δεδομένων είναι υποχρεωτική. Για να είναι ολοκληρωμένη η προστασία εκτός από την εγκατάσταση των προγραμμάτων απαιτείται διαρκής ενημέρωση. Ένα από τα πιο σημαντικά κριτήρια επιλογής Internet firewall θα πρέπει να είναι οι λεγόμενες λειτουργίες ελέγχου της εξερχόμενης κυκλοφορίας (traffic), δίνοντάς στο χρήστη επιλογές αποδοχής, απόρριψης της αποστολής των packets (Κάθε αρχείο που αποστέλλεται μέσω του δικτύου τεμαχίζεται σε packets έτσι ώστε να είναι πιο γρήγορη και πιο ευέλικτη η μεταφορά τους που επιχειρεί να στείλει μια εφαρμογή). Ακόμα και τα πιο ακραία μέτρα ασφαλείας δεν μπορούν να εγγυηθούν την απόλυτη ασφάλεια. Έτσι, για την επίτευξη της σχετικής ασφάλειας απαιτείται η τήρηση μια σειρά κανόνων, συγκεκριμένα:

1. Επιλογή ενός καλού antivirus προγράμματος.
2. Τακτική ανίχνευση όλου του δίσκου με το antivirus.
3. Συνεχής ανανέωση (update) του.
4. Έλεγχος κάθε δισκέτας/cd με το antivirus πριν την ανοίξει ο χρήστης.
5. Τήρηση αντιγράφων ασφαλείας όλων των αρχείων του σε cd ή δισκέτα.
6. Συχνές επισκέψεις στην τοποθεσία των κρίσιμων ενημερώσεων των Windows (το πιο ευάλωτο λειτουργικό) όπου προσφέρονται δωρεάν προγράμματα (patches) διόρθωσης/κάλυψης των πιθανών ελλείψεων του λειτουργικού του. Η πιο έγκυρη πηγή ενημέρωσης είναι το Microsoft TechNet (www.microsoft.com/technet). Μπορεί ο κάθε χρήστης να το επισκεφθεί και να κάνει κλικ στο Click on Hotfix & Bulletin Search για να δει για ποια προγράμματα χρειάζεται patches και ποια όχι
7. Ανίχνευση μέσω του αντιβιοτικού κάθε νέου αρχείου που «κατεβάζει» από το Internet.
8. Αν χρησιμοποιεί irc chat, τότε να απενεργοποιήσει την επιλογή αυτόματης

αποδοχής αρχείων και αυτόματης εκτέλεσης των αρχείων που του στέλνουν.
9. Να επιλέξει την πλήρη εμφάνιση των τύπων αρχείων στον Η/Υ του. Ίσως κάποιος να του στείλει μια «φωτογραφία» ως photo.jpg.vbs. Αν δεν έχει την παραπάνω επιλογή ενεργοποιημένη, θα εκτελέσει το αρχείο το οποίο θα περιέχει κάθε άλλο παρά φωτογραφία.
10. Να διατηρεί και να ανανεώνει συχνά μια δισκέτα για αποκατάσταση ζημιών από ιούς, την οποία προσφέρουν συνήθως τα ίδια τα αντιβιοτικά προγράμματα.
11. Διατήρηση της ανωνυμίας του με την ενημέρωση του browser που χρησιμοποιεί. Να προτιμάτε πάντα την πιο πρόσφατη έκδοση και φυσικά να φροντίζει να την ενημερώνει τακτικά με όλα τα security patches.
12. Σωστή ρύθμιση των δικτυακών εφαρμογών. Οι περισσότεροι Web browsers διαθέτουν ρυθμίσεις ασφαλείας που καθορίζουν ποια components, ποια Java applets ή άλλα στοιχεία των web sites μπορούν να «εκτελεστούν» από τον browser, ενώ επιτρέπουν πλέον και μια πιο έξυπνη και ασφαλή διαχείριση των cookies. Οι χρήστες των Windows μπορούν να στραφούν επιπλέον στη χρήση του Microsoft Baseline Security Analyzer. Πρόκειται για ένα δωρεάν διαθέσιμο από το TechNet εργαλείο που ελέγχει το σύστημά για κακές ρυθμίσεις.
13. Αν χρησιμοποιεί instant messengers, να αποφεύγει να συνομιλεί με ξένους.
14. Εδώ πρέπει να επισημανθεί πως όσο πιο αυστηρές ρυθμίσεις ασφαλείας ενεργοποιούνται στον υπολογιστή, τόσο πιο δύσκολη γίνεται και η πρόσβαση σε σελίδες του Διαδικτύου. Η συνήθης ρύθμιση ασφαλείας στους φυλλομετρητές είναι η «μεσαία».

ΕΠΙΛΟΓΟΣοΕ

Στη σύγχρονη εποχή της πληροφορίας, του Διαδικτύου και της κοινωνικής δικτύωσης, έχουν γεννηθεί πολυποίκιλες ευκαιρίες για εγκληματική δράση. Παραδοσιακώς τελούμενα εγκλήματα, όπως αυτό της σεξουαλικής παρενόχλησης, της παιδικής πορνογραφίας, των οικονομικών απατών, της παρενόχλησης, του οργανωμένου εγκλήματος, της τρομοκρατίας, χρησιμοποιούν σαν δούρειο ίππο τα νέα τεχνολογικά επιτεύγματα και μετεξελίσσονται στο χώρο και στο χρόνο. Παράλληλα, νέες μορφές εγκληματικών συμπεριφορών (hacking, virus & malware infection, espionage, cracking and Distributing Denial of Service attacks) αναφύονται και σε συνδυασμό με τα προαναφερθέντα συγκροτούν τη νεοεκκολαφθείσα κατηγορία των ηλεκτρονικών εγκλημάτων.

Ο όρος «ηλεκτρονικό έγκλημα» δεν απηχεί κοινού νομικού ή επιστημονικού ορισμού. Σύμφωνα με τον Wall (2011), «κάθε πράξη ή παράλειψη που διαπράττεται σε παγκόσμιο πληροφοριακό επίπεδο με τη βοήθεια του διαδικτύου» μπορεί να οριστεί ως ηλεκτρονικό έγκλημα. Τα ηλεκτρονικά εγκλήματα δύνανται να λαμβάνουν ποικίλες κατηγοριοποιήσεις και ταξινομήσεις, με πιο διαδεδομένη αυτή που προκύπτει από τη Σύμβαση του Συμβουλίου της Ευρώπης το 2001 και η οποία και τα χωρίζει σε τέσσερις μεγάλες κατηγορίες: 1) Εγκλήματα κατά της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας δεδομένων ηλεκτρονικών υπολογιστών (αδικήματα μορφής CIA). 2) Εγκλήματα σχετιζόμενα με ηλεκτρονικούς υπολογιστές, που διαπράττονται μέσω αυτών. 3) Εγκλήματα που χαρακτηρίζονται από το παράνομο περιεχόμενό τους, το οποίο και διανέμεται μέσω του διαδικτύου και 4) Εγκλήματα σχετικά με την προσβολή της πνευματικής ιδιοκτησίας. Σύμφωνα με την Ελληνική Αστυνομία (2016) οι κυριότερες μορφές των ηλεκτρονικών εγκλημάτων, που εξιχνιάσθηκαν στην Ελλάδα από το Τμήμα Ηλεκτρονικού Εγκλήματος/ΔΑΑ, είναι οι απάτες μέσω διαδικτύου, η παιδική πορνογραφία, η διακίνηση και πειρατεία λογισμικού, οι κακόβουλες εισβολές σε δίκτυα (hacking), οι απάτες με πιστωτικές κάρτες, η διακίνηση ναρκωτικών καθώς και ο διαδικτυακός εκφοβισμός που απαντάται συνήθως στα μέσα κοινωνικής δικτύωσης και γενικότερα τα εγκλήματα στα chat rooms.

Η ύπαρξη ενός ατόμου με κίνητρο να διαπράξει έγκλημα, ενός κατάλληλου και ευάλωτου στόχου καθώς και η απουσία αποτελεσματικού ελέγχου/αστυνόμευσης είναι τρεις βασικές προϋποθέσεις, που όντας ταυτόχρονα παρούσες χωρικά και χρονικά, δύναται να οδηγήσουν στην εμφάνιση ποινικά κολάσιμων συμπεριφορών τόσο εντός όσο και εκτός της διαδικτυακής ζωής. Το γεγονός ότι το ίδιο το διαδίκτυο είναι εξ υπάρξεώς του «εγκληματογόνο», όπως χαρακτηριστικά αναφέρουν οι Newman & Clarke (2003), ενισχύεται και από τα εγγενή χαρακτηριστικά του, τα οποία και συμβάλλουν στη ραγδαία αύξηση του ηλεκτρονικού εγκλήματος και συνοψίζονται ως κάτωθι:

- Το διαδίκτυο προσφέρει «ανωνυμία» για τον εκάστοτε χρήστη. Έτσι, ο εκάστοτε εγκληματίας αισθάνεται πιο ελεύθερος και ασφαλής πίσω από μια ψεύτικη ταυτότητα, παραμένοντας αόρατος κατά τη διάπραξή του και αφήνοντας

ελάχιστα ή και καθόλου ψηφιακά ίχνη τέλεσης του εγκλήματός του, δυσχεραίνοντας έτσι κατά πολύ το έργο των διωκτικών αρχών.

- Το γεγονός ότι κάθε άτομο μπορεί να έχει εύκολη και με χαμηλό κόστος εικοσιτετράωρη πρόσβαση σε μια πηγή απεριορίστων, παντός τύπου πληροφοριών, εφαρμογών και δραστηριοτήτων, όπως το Διαδίκτυο, δημιουργεί έδαφος για ποικίλες εγκληματικές συμπεριφορές. Εγκλήματα μπορεί να τελούνται από τον προσωπικό χώρο των δραστών με χρήση μόνο ενός υπολογιστή και σε χρόνο δευτερολέπτων, χωρίς πολλές φορές να γίνονται αντιληπτά από τα ίδια τα θύματα.
- Μέσω του διαδικτύου, συγκεκριμένες ομάδες δραστών με κοινό στόχο μπορούν να επικοινωνούν άμεσα και δη σε πραγματικό χρόνο, χωρίς επιπρόσθετες μετακινήσεις, ανταλλάσσοντας απόψεις και γενικότερα συζητώντας σε chat rooms, blogs και μέσα κοινωνικής δικτύωσης, εμπλουτίζοντας έτσι το Modus operandi τους και εμπλουτίζοντας τις γνώσεις τους μα και την εγκληματική δράση τους μέσω των διαδικτυακών συνεργών τους.
- Λόγω της παγκόσμιας φύσης του διαδικτύου και της απουσίας φυσικών και γεωγραφικών ορίων, είναι πολύ δύσκολο να προσδιοριστεί ο τόπος και ο ακριβής χρόνος τέλεσης των εγκλημάτων που διαπράττονται στον Κυβερνοχώρο, με αρκετά δύσκολη και τη διερεύνηση και τον εντοπισμό των δραστών. Επιπροσθέτως, εξαιτίας αυτής της παγκόσμιας διασύνδεσης των πληροφοριακών συστημάτων, ο δράστης μπορεί να ανακαλύψει ακόμη πιο εύκολα την «αχίλλειο πτέρνα» τους και να εξαπολύσει την όποια επίθεση εναντίον τους.
- Η ολοένα μεταβαλλόμενη και εξελισσόμενη φύση του διαδικτύου σε τεχνολογικό και γνωστικό επίπεδο, καθιστά απαραίτητη την εξειδικευμένη εκπαίδευση των μονάδων δίωξης ηλεκτρονικών εγκλημάτων σε θεωρητικό και πρακτικό επίπεδο.
- Η απουσία ουσιαστικού, κοινού διαδικτυακού ελέγχου καθώς και η έλλειψη ενιαίου νομοθετικού πλαισίου σε παγκόσμιο επίπεδο καθιστά δυσχερή την ποινική αντιμετώπιση κολάσιμων συμπεριφορών, τόσο διασυνοριακά όσο και μέσα σε μια επικράτεια.

Εξαιτίας όλων των προαναφερθέντων, θύματα ηλεκτρονικών εγκλημάτων διστάζουν να αποκαλύψουν και να καταγγείλουν την όποια εγκληματική εις βάρος τους συμπεριφορά, με αποτέλεσμα το μέγεθος της εγκληματικότητας στο χώρο του Διαδικτύου να είναι «ακόμα πιο σκοτεινό» από ότι στον «κοινό» εγκληματικό χώρο.

Τα ηλεκτρονικά εγκλήματα έχουν αυξηθεί κατά πολύ τα τελευταία χρόνια. Σύμφωνα με τη μελέτη ηλεκτρονικού εγκλήματος από τη Norton το 2011, από το 2010 μέχρι και το 2011 σε 24 χώρες, κάθε δευτερόλεπτο 14 ενήλικες γίνονταν θύματα ηλεκτρονικών εγκλημάτων, αριθμός που ανέρχεται σε πάνω από 1 εκατομμύριο θύματα την ημέρα. Μια μεταγενέστερη μελέτη του ίδιου οργανισμού το 2016, αποκάλυψε ότι το 2015, 594 εκατομμύρια άνθρωποι παγκοσμίως είχαν βιώσει έστω και μία κακόβουλη διαδικτυακή επίθεση, με τα θύματα καθημερινά να υπολογίζονται σε 1,5 εκατομμύρια άτομα, ενώ υπολογίστηκε ότι έχουν χαθεί πάνω από 150 δισεκατομμύρια δολάρια εξαιτίας οικονομικών ηλεκτρονικών απατών. Η

αναγκαιότητα αντιμετώπισης των ηλεκτρονικών εγκλημάτων ενισχύεται και από την τελευταία Οικονομοτεχνική Ανάλυση της PWC του 2016, η οποία σε έρευνα στον επιχειρηματικό χώρο κατέγραψε ότι το 1/3 των 6.000 και πλέον συμμετεχουσών στην έρευνα επιχειρήσεων είχαν έρθει αντιμέτωποι με κάποιου είδους διαδικτυακό έγκλημα οικονομικής φύσεως, με ζημιές που πολλές φορές ξεπερνούσαν τα 100 εκατομμύρια δολάρια.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Βλαχόπουλου Κ., Ηλεκτρονικό Έγκλημα, Εκδ. Νομική Βιβλιοθήκη 2007

2. Κιούπη Δ., Ηλεκτρονικά Οικονομικά Εγκλήματα,

3. Λάζος Γ. Πληροφορική και έγκλημα , Εκδόσεις Νομική Βιβλιοθήκη , Αθήνα 2001.

4. Μαρκοπούλου Παγώνα, Η Σύμβαση για το Κυβερνοέγκλημα, 2008

5. Δημήτριος Μ. Πουλάκης, Κρυπτογραφία, η επιστήμη της ασφαλούς επικοινωνίας, Εκδόσεις Ζήτη, Δεκέμβριος 2005.

6. Nigel Smart, Cryptography: An Introduction, McGraw-Hill Education, November 2002.

7. Douglas Stinson, Cryptography: Theory and Practice (Discrete Mathematics & Its Applications S.), CRC Press, February 27, 2002.

8. Δημήτρης Γκριτζαλης, Στέφανος Γκριτζαλης, Σωκράτη Κατσικα, Ασφάλεια Δικτύων υπολογιστών, Εκδόσεις Παπασωτηριου 2003

9. Νικολαΐδης Χρ.(1999), «Η σκοτεινή πλευρά του Internet», Αθήνα, Εκδ.Anubis.

10. Ζάννη Αν.(2005), «Το διαδικτυακό έγκλημα, Αθήνα», Αντ. Ν. Σάκκουλας.

11. ΓΚΡΙΤΖΑΛΗ Δ. ,(2004) Ασφάλεια και πολιτική ανυπακοή στον Κυβερνοχώρο

12. "ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ΚΑΙ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ"

Άρης Αλεξόπουλος, Γιώργος Λαγογιάννης

13. Τι είναι και πως δουλεύει το Tor για Ανωνυμία στο διαδίκτυο

14. http://www.anonymizer.com/
15. http://www.billssoftwarepicks.com/software/connectivity/network_monitors/.
16 http://www.freedom.net/
17. http://freenet.sourceforge.net/