ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΔΥΤΙΚΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

Πτυχιακή Εργασία

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ

ΟΜΑΔΑ ΣΠΟΥΔΑΣΤΩΝ:

ΔΡΟΥΓΟΥΤΗΣ ΠΑΝΑΓΙΩΤΗΣ

ΟΡΛΩΦ ΓΙΑΝΝΗΣ

ΤΣΟΥΚΑΛΑΣ ΑΓΓΕΛΟΣ

ΕΠΟΠΤΕΥΩΝ ΚΑΘΗΓΗΤΗΣ:ΑΡΗΣ ΜΠΑΚΑΛΗΣ

ΠΑΤΡΑ 2014

Contents

1 ΕΙΣΑΓΩΓΗ

Καθένας από τους τρεις προηγούμενους αιώνες χαρακτηρίζεται και από μια τεχνολογική ανακάλυψη. Ο 18ος ήταν ο αιώνας των μεγάλων μηχανικών συστημάτων, που συνόδευσαν τη βιομηχανική επανάσταση. Ο 19ος ήταν ο αιώνας της ατμομηχανής. Κατά τη διάρκεια του 20ου αιώνα, το κλειδί της τεχνολογίας ήταν η συγκέντρωση, η επεξεργασία και η κατανομή της πληροφορίας. Ανάμεσα σε άλλες εξελίξεις, παρατηρούμε την εγκατάσταση διεθνών τηλεφωνικών δικτύων, την ανακάλυψη του ραδιοφώνου και της τηλεόρασης, τη γέννηση και την άνευ προηγουμένου ανάπτυξη της βιομηχανίας των ηλεκτρονικών υπολογιστών και την εκτόξευση των τηλεπικοινωνιακών δορυφόρων.

Κατά το τέλος του 20ου αιώνα, αυτές οι περιοχές συγκλίνουν γρήγορα και οι διαφορές ανάμεσα στη συγκέντρωση, μεταφορά, αποθήκευση και επεξεργασία της πληροφορίας γρήγορα εξαφανίζονται. Οργανισμοί με εκατοντάδες γραφεία, διασκορπισμένα σε μια μεγάλη γεωγραφική περιοχή, είναι πλέον συνηθισμένο να απαιτούν να έχουν τη δυνατότητα ελέγχου της τρέχουσας κατάστασης και στα πλέον απομακρυσμένα γραφεία τους με το πάτημα ενός κουμπιού. Το παλιό μοντέλο του μοναδικού υπολογιστή που εξυπηρετεί όλες τις υπολογιστικές ανάγκες ενός οργανισμού έχει αντικατασταθεί με γρήγορο ρυθμό από ένα μοντέλο, στο οποίο ένας μεγάλος αριθμός από ξεχωριστούς, αλλά συνδεδεμένους μεταξύ τους υπολογιστές. Τα συστήματα αυτά ονομάζονται δίκτυα υπολογιστών (computernetworks).

Παλιά στις πρώτες μέρες των υπολογιστών, όταν εταιρίες και πανεπιστήμια είχαν ένα απομονωμένο υπολογιστικό κέντρο, η επίτευξη της ασφάλειας ήταν μια εύκολη υπόθεση. Αρκούσε απλά και μόνο ένας φύλακας στην πόρτα του δωματίου, όπου υπήρχε ο υπολογιστής, ο οποίος εξασφάλιζε ότι κανείς δεν θα έπαιρνε ταινίες, δίσκους ή κάρτες από το δωμάτιο. Με την εμφάνιση των δικτύων, η κατάσταση

άλλαξε ριζικά. Κανείς δεν μπορεί να αστυνομεύσει με φυσικά μέσα τα εκατομμύρια bits των δεδομένων που μετακινούνται καθημερινά μεταξύ των υπολογιστών σε ένα δίκτυο. Ακόμα περισσότερο, οι οργανισμοί δεν μπορούν να είναι σίγουροι ότι τα δεδομένα τους δεν αντιγράφηκαν μυστικά με υποκλοπή ή άλλα μέσα κατά τη διαδρομή προς τον σωστό προορισμό τους. Οι υποκλοπές είναι ένα πολύ πιο συνηθισμένο γεγονός από ό,τι αντιλαμβάνονται οι περισσότεροι άνθρωποι. Τα πράγματα γίνονται χειρότερα όταν τα δεδομένα μεταφέρονται μέσω δορυφορικών ζεύξεων, οπότε γίνονται διαθέσιμα σε οποιονδήποτε κάνει τον κόπο να στήσει μια κεραία για να ακροαστεί. Σαφώς απαιτείται κάποιο είδος κρυπτογράφησης (encryption) για να καταστήσεις τα δεδομένα ακατανόητα για όλους, εκτός του προοριζόμενου δέκτη.

Η προστασία των δεδομένων από αδιάκριτα μάτια δεν είναι το μόνο θέμα ασφάλειας στη δικτύωση. Μπορεί κανείς να φανταστεί τουλάχιστον τέσσερις υπηρεσίες ασφάλειας:

1. Προστασία δεδομένων για να μην αναγνωστούν από μη εξουσιοδοτημένα άτομα
2. Παρεμπόδιση μη εξουσιοδοτημένων ατόμων από το να εισάγουν ή να διαγράφουν μηνύματα
3. Επιβεβαίωση της ταυτότητας του αποστολέα κάθε μηνύματος
4. Παροχή δυνατότητας σε χρήστες να στέλνουν υπογεγραμμένα έγγραφα με ηλεκτρονικό τρόπο.

Γενικά, λοιπόν, γίνεται αντιληπτό ότι το θέμα της ασφάλειας των ηλεκτρονικών δεδομένων, ηλεκτρονικής επικοινωνίας και συναλλαγών αποτελεί ένα μείζον θέμα τόσο για όλους τους οργανισμούς, αλλά και τις επιχειρήσεις.

2 ΕΙΔΗ ΔΙΚΤΥΩΝ

2.1 Δίκτυα επιχειρήσεων/οργανισμών/εταιριών

Ο συνεχώς αυξανόμενος ανταγωνισμός στον τομέα των επιχειρήσεων έχει πλέον επιβάλει τη χρήση ηλεκτρονικών υπολογιστών, καθώς από αυτούς εξαρτάται η βιώσιμη ανάπτυξη και η εξέλιξη της κάθε επιχείρησης. Σήμερα υπάρχουν πολλές εταιρίες που έχουν σημαντικό αριθμό υπολογιστών, οι οποίοι λειτουργούν είτε σε μικρή απόσταση είτε σε μεγάλες αποστάσεις μεταξύ τους. Για παράδειγμα, μια εταιρεία με πολλά εργοστάσια μπορεί να έχει έναν υπολογιστή σε κάθε μέρος για να κρατά στοιχεία που έχουν να κάνουν με τα αποθέματα, να παρακολουθεί την παραγωγικότητα και να διεκπεραιώνει διάφορες εργασίες όπως η τοπική μισθοδοσία.

Στα μοντέλα των υπολογιστικών συστημάτων που χρησιμοποιήθηκαν πρώτα από τις διάφορες επιχειρήσεις μπορούσε να αξιοποιηθεί ο κάθε υπολογιστής χωριστά από όλους τους υπόλοιπους. Καθώς, όμως, οι τηλεπικοινωνίες και η πληροφορική αναπτύχθηκαν αλματωδώς, οι μικρές και μεσαίες επιχειρήσεις απέκτησαν άμεση πρόσβαση στην πληροφορία, γεγονός που αύξησε τη δυναμική τους, αλλά ταυτόχρονα δημιούργησε το πρόβλημα της ύπαρξης ορθού καταμερισμού των πόρων. Τότε οι διοικήσεις των επιχειρήσεων αποφάσισαν να υπάρξει διασύνδεση όλων των υπολογιστών, ώστε όλοι να έχουν πρόσβαση στην πληροφορία και τον εξοπλισμό και να αποκτήσουν τη δυνατότητα εξαγωγής και συσχέτισης πληροφοριών που αφορούν ολόκληρη την επιχείρηση.

Η ασφάλεια της διατήρησης των δεδομένων μιας επιχείρησης είναι ένα πολύ σημαντικό ζήτημα για αυτήν, καθώς εμπίπτει σε θέματα υψηλής αξιοπιστίας που παρέχει το δίκτυό της. Για να επιτευχθεί αυτό απαιτούνται εναλλακτικές πηγές τροφοδοσίας, οι οποίες μπορούν να λειτουργούν ακόμα και όταν κάποια μονάδα βγει εκτός λειτουργίας.

Μια επιχείρηση με κερδοσκοπικό χαρακτήρα αλλά και ένας οργανισμός με μεγάλο αριθμό εργαζομένων/υπολογιστικών μονάδων ενδιαφέρονται σε μεγάλο βαθμό για την εξοικονόμηση χρημάτων. Ως γνωστόν, ένας μικρός υπολογιστής έχει καλύτερο λόγο κόστους/επίδοση από έναν μεγαλύτερο υπολογιστή. Από την άλλη πλευρά, ένας μεγάλος υπολογιστής είναι πολύ ταχύτερος από έναν προσωπικό υπολογιστή, αλλά κοστίζει πολύ περισσότερο. Λόγω του ότι υπάρχει αυτή η ανισορροπία, πολλές επιχειρήσεις που έχουν προσωπικούς υπολογιστές (έναν ανά χρήστη), κρατούν τα σημαντικά δεδομένα σε έναν ή περισσότερους κοινόχρηστους υπολογιστές (μοντέλο πελάτη-εξυπηρετητή).

Ένας επιπρόσθετος στόχος της δικτύωσης θα μπορούσαμε να πούμε ότι είναι και η ικανότητα βαθμιαίας αύξησης της επίδοσης του συστήματος, καθώς αυξάνει το φορτίο, με απλή πρόσθεση περισσοτέρων επεξεργαστών. Τέλος, ένα ακόμα κέρδος που έχει μια επιχείρηση ή μια εταιρεία από την εγκατάσταση δικτύων υπολογιστών στους χώρους δραστηριοποίησής της, είναι ότι οι εργαζόμενοι έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους άμεσα ακόμη και αν βρίσκονται σε μεγάλες αποστάσεις και να διεκπεραιώνουν εργασίες που απαιτούν ομαδική συμβολή και προσπάθεια για την επίτευξη των στόχων της επιχείρησης και που σε αντίθετη περίπτωση είναι χρονοβόρες και πολλές φορές μη αποδοτικές.

2.2 **Οικιακά δίκτυα**

Αν και η εγκατάσταση δικτύων υπολογιστών σε μια επιχείρηση ή εταιρία διέπεται κυρίως από τεχνολογικά και οικονομικά κριτήρια, αυτά έγιναν δημοφιλή όταν τα δίκτυα προσωπικών υπολογιστών άρχισαν να προσφέρουν μεγαλύτερο πλεονέκτημα κόστους προς επίδοση, σε σχέση με τους μεγάλους υπολογιστές.

Τα δίκτυα υπολογιστών άρχισαν να παρέχουν υπηρεσίες σε ιδιώτες, με την μορφή τοπικών οικιακών δικτύων, στις αρχές της δεκαετίας του 1990. Τέτοιες υπηρεσίες

είναι η πρόσβαση σε απομακρυσμένες πληροφορίες, η επικοινωνία πρόσωπο με πρόσωπο καθώς και η διασκέδαση με αλληλεπίδραση.

Η πρόσβαση σε απομακρυσμένες πληροφορίες έχει πολλές μορφές. Είναι μια πραγματικότητα το ότι πολλοί άνθρωποι διεκπεραιώνουν τις τραπεζικές τους συναλλαγές αλλά και τις αγορές τους με ηλεκτρονικό τρόπο ενώ οι κατάλογοι των προϊόντων και των υπηρεσιών που μπορεί κανείς να βρει μέσω του διαδικτύου συνεχώς εμπλουτίζονται και γίνονται πιο δελεαστικοί. Η πρόσβαση στην ενημέρωση και την πληροφόρηση έχει γίνει πιο εύκολη από ποτέ μέσω του ηλεκτρονικού τύπου, ενώ παραδοσιακές συνήθειες όπως η αναζήτηση ενός καλού βιβλίου στα ράφια κάποιου βιβλιοπωλείου έχουν αντικατασταθεί από την αναζήτηση μεταξύ χιλιάδων τίτλων και την σχεδόν ακαριαία εύρεση του τίτλου που μας ενδιαφέρει στα ‘ράφια’ ενός εικονικού βιβλιοπωλείου.

Η δεύτερη ευρεία κατηγορία χρήσης των δικτύων είναι για διαλόγους πρόσωπο με πρόσωπο. Χαρακτηριστικό παράδειγμα αποτελεί το ηλεκτρονικό ταχυδρομείο το οποίο χρησιμοποιείται από εκατομμύρια ανθρώπων και επιτρέπει πλέον και την μεταφορά ήχου και εικόνας πέραν του κειμένου. Με αυτόν τον τρόπο δίνεται η δυνατότητα στους χρήστες να πραγματοποιούν τηλεδιασκέψεις και να επικοινωνούν χωρίς καθυστερήσεις ενώ σημαντικές εφαρμογές κοινωνικού χαρακτήρα όπως η λήψη ιατρικών διαγνώσεων από ειδικούς σε απομακρυσμένες περιοχές αλλά και η εκπαίδευση από απόσταση. Στην κατηγορία αυτή των υπηρεσιών ανήκουν και τα λεγόμενα ‘φόρουμ’ στα οποία ο οποιοσδήποτε μπορεί συμμετάσχει ανταλλάσοντας απόψεις πάνω σε θέματα που τον αφορούν. Η θεματολογία των χώρων αυτών ηλεκτρονικής συζήτησης είναι τόσο ευρεία που η διάδοσή τους υπήρξε ραγδαία και συνεχής.

Στην τρίτη κατηγορία υπηρεσιών όπως αναφέραμε στην αρχή ανήκουν οι υπηρεσίες διασκέδασης με αλληλεπίδραση. Πρόκειται ίσως για την πιο ταχέως αναπτυσσόμενη βιομηχανία όπου δίδει στον χρήστη την δυνατότητα από την

οθόνη του υπολογιστή του να επιλέγει την ταινία που επιθυμεί να δει, το τραγούδι που θέλει να ακούσει, το παιχνίδι που θέλει να παίξει και μέσα σε λίγα λεπτά να το έχει στον υπολογιστή του έναντι ενός ιδιαιτέρως χαμηλού ποσού. Στην περίπτωση δε που μιλάμε για ηλεκτρονικά παιχνίδια τότε η εγκατάσταση δικτύου υπολογιστών απογειώνει την ευχαρίστηση των φανατικών του είδους.

2.3 **Κατηγορίες δικτύων**

Η ταξινόμηση των δικτύων κρίνεται αναγκαία, λόγω της μεγάλης διάδοσής τους, ανάλογα με τις εφαρμογές τους και βάσει των τεχνικών χαρακτηριστικών τους. Γενικά, δεν υπάρχει μια γενικά ταξινόμηση στην οποία να ταιριάζουν όλα τα δίκτυα. Εντούτοις, δύο χαρακτηριστικά των δικτύων που τα ξεχωρίζουν ως ιδιαιτέρως σημαντικά, είναι η τεχνολογία μετάδοσης και η κλίμακα.

Η τεχνολογία μετάδοσης στα δίκτυα υπολογιστών γίνεται με δύο τρόπους, με τα Δίκτυα Εκπομπής και με τα Δίκτυα Σημείου προς Σημείου.

Τα Δίκτυα Εκπομπής έχουν έναν μοναδικό δίαυλο επικοινωνίας που τον μοιράζονται όλες οι μηχανές του δικτύου. Ένας υπολογιστής ενός τέτοιου δικτύου αποστέλλει μηνύματα με την μορφή πακέτων στο δίκτυο και αυτά λαμβάνονται από όλους τους υπόλοιπους υπολογιστές του δικτύου. Με την παραλαβή του πακέτου κάθε υπολογιστής εξετάζει το πεδίο διεύθυνσης που αναγράφεται πάνω στο κάθε πακέτο και το οποίο είναι χαρακτηριστικό του τελικού προορισμού του. Αν το πακέτο προορίζεται για αυτόν τότε το επεξεργάζεται, αλλιώς το αγνοεί. Στα δίκτυα εκπομπής υπάρχει και η δυνατότητα της αποστολής ενός πακέτου σε όλα τα μέλη του δικτύου χρησιμοποιώντας κατάλληλο κωδικό στο πεδίο της διεύθυνσης του πακέτου, οπότε όλοι οι υπολογιστές του συγκεκριμένου δικτύου έχουν τη δυνατότητα να επεξεργαστούν την ίδια πληροφορία. Σε αυτήν τη περίπτωση μιλάμε για λειτουργία εκπομπής. Μερικά συστήματα εκπομπής υποστηρίζουν την

μετάδοση σε ένα υποσύνολο υπολογιστών που ανήκουν σε ένα δίκτυο, οπότε μιλάμε για πολλαπλή διανομή, και αυτό γίνεται εφικτό αφιερώνοντας ένα bit διεύθυνσης ώστε να φανερώνει πολλαπλή διανομή.

Από την άλλη πλευρά, στα Δίκτυα Σημείου προς Σημείο έχουμε πολλές συνδέσεις μεταξύ συγκεκριμένων ζευγών μηχανών. Κατά την διαδικασία μετάβασης ενός πακέτου από την πηγή στον προορισμό θα πρέπει να γίνεται σωστή επιλογή του υπολογιστή στον οποίο κατευθύνεται το πακέτο μιας και περνάει από διάφορους ενδιάμεσους υπολογιστές, καθώς και ορθή επιλογή της διαδρομής που θα ακολουθήσει το πακέτο μιας και συνήθως υπάρχουν πολλαπλές διαδρομές διαφορετικού μήκους μεταξύ των οποίων καλείται ο αλγόριθμος δρομολόγησης να επιλέξει.

Γενικά θα μπορούσαμε να πούμε ότι τα μικρότερα και γεωγραφικά περιορισμένα δίκτυα τείνουν να χρησιμοποιούν την εκπομπή, ενώ τα μεγαλύτερα δίκτυα είναι συνήθως σημείου προς σημείου.

Τα δίκτυα ταξινομούνται με βάση την κλίμακά τους. Στην κορυφή αυτής της ιεραρχίας υπάρχουν οι μηχανές ροής δεδομένων, δηλαδή υπολογιστές που διαθέτουν πολλές λειτουργικές μονάδες οι οποίες δουλεύουν για το ίδιο πρόγραμμα. Μετά συναντάμε τους πολλαπλούς υπολογιστές, που είναι συστήματα τα οποία επικοινωνούν μεταξύ τους στέλνοντας μηνύματα μέσω μικρών και πολύ γρήγορων αρτηριών. Στη συνέχεια έχουμε τα αληθινά δίκτυα, στα οποία για να επικοινωνήσουν οι υπολογιστές, ανταλλάσουν μηνύματα μέσω καλωδίων μεγαλύτερου μήκους. Διαιρούνται σε τοπικά, μητροπολιτικά και ευρείας περιοχής, ενώ η σύνδεση δύο ή περισσοτέρων δικτύων ονομάζεται διαδίκτυο. Η απόσταση στην οποία εκτείνεται το καθένα από τα παραπάνω είναι σημαντική επειδή χρησιμοποιούνται διαφορετικές τεχνικές σε διαφορετικές κλίμακες και για τον λόγο αυτό παραθέτουμε τον παρακάτω πίνακα 1.

Απόσταση μεταξύ επεξεργαστών	Θέση Επεξεργαστών	Παραδείγματα
0,1m	στην ίδια κάρτα	Μηχανή ροής δεδομένων
1m	στο ίδιο σύστημα	Πολλαπλός υπολογιστής
10m	στο ίδιο δωμάτιο	Τοπικό δίκτυο
100m	στο ίδιο κτίριο	Τοπικό δίκτυο
1km	στην ίδια περιοχή	Τοπικό δίκτυο
10km	στην ίδια πόλη	Μητροπολιτικό δίκτυο
100km	στην ίδια χώρα	Δίκτυο Ευρείας Περιοχής
1000km	στην ίδια Ήπειρο	Δίκτυο Ευρείας Περιοχής
10000km	στον ίδιο πλανήτη	Το Διαδίκτυο

Πίνακας 1.

2.3.1 **Τοπικά δίκτυα**

Τα Τοπικά Δίκτυα (local area networks ή LAN) είναι ιδιωτικά δίκτυα που στεγάζονται σε ένα και μοναδικό κτίριο ή σε εγκαταστάσεις ακτίνας έως μερικά χιλιόμετρα. Με τα τοπικά δίκτυα συνδέονται προσωπικοί υπολογιστές και σταθμοί εργασίας σε γραφεία εταιρειών με σκοπό την κοινή χρήση των περιφερειακών και την ανταλλαγή πληροφοριών. Τα LAN διακρίνονται από τα άλλα είδη δικτύων με βάση το μέγεθος, την τεχνολογία μετάδοσης και την τοπολογία τους.

Όσον αφορά στο μέγεθός τους, τα τοπικά δίκτυα συνήθως είναι περιορισμένου μεγέθους με αποτέλεσμα ο χρόνος μετάδοσης να είναι γνωστός εκ των προτέρων.

Ως προς την τοπολογία του δικτύου συναντάμε διάφορες γεωμετρίες. Οι δύο πιο γνωστές είναι το *δίκτυο αρτηρίας* και ο *δακτύλιος*. Σε ένα *δίκτυο αρτηρίας* η άδεια μετάδοσης δίνεται μόνο από έναν υπολογιστή, ο οποίος είναι αυτός που εξουσιάζει το δίκτυο. Όταν άλλοι υπολογιστές επιδιώξουν να έχουν και αυτοί άδεια μετάδοσης, τότε απαιτείται να υπάρχει ένας μηχανισμός διαιτησίας, ώστε να επιλύονται οι ενδιάμεσες συγκρούσεις μεταξύ των υπολογιστών. Αντίθετα, σε ένα *δίκτυο δακτυλίου* κάθε bit διαδίδεται μόνο του χωρίς να περιμένει το υπόλοιπο πακέτο στο οποίο ανήκει, ενώ κάνει τον γύρο ολόκληρου του δακτυλίου σε χρόνο που απαιτείται για την μετάδοση ολίγων bit συχνά πριν ακόμη μεταδοθεί ολόκληρο το πακέτο.

2.3.2 **Μητροπολιτικά δίκτυα**

Ένα Μητροπολιτικό Δίκτυο (metropolitanareanetwork ή MAN) είναι μια μεγαλύτερη εκδοχή ενός τοπικού δικτύου και συνήθως χρησιμοποιεί παρόμοια τεχνολογία. Μπορεί να καλύπτει ομάδα γειτονικών γραφείων μιας επιχείρησης ή μια πόλη και μπορεί να είναι είτε ιδιωτικό είτε δημόσιο. Ένα μητροπολιτικό δίκτυο μπορεί να υποστηρίζει δεδομένα καθώς και φωνή και ίσως ακόμη να σχετίζεται με την καλωδιακή τηλεόραση. Το μητροπολιτικό δίκτυο χρησιμοποιεί ένα ή δύο καλώδια και δεν διαθέτει στοιχεία μεταγωγής που να διοδεύουν τα πακέτα προς τη μια από τις πολλές διαφορετικές γραμμές εξόδου.

2.3.3 **Διαδίκτυο**

Ως διαδίκτυο (Internet) εννοείται κάθε συνένωση δύο ή περισσοτέρων δικτύων, όχι κατ' ανάγκη ίδιας τεχνολογίας, έτσι ώστε να επιτυγχάνεται η επικοινωνία μεταξύ τους και να λειτουργούν σαν ένα δίκτυο. Για να δικτυωθούν τα επιμέρους δίκτυα χρησιμοποιούνται συσκευές τηλεπικοινωνιών, όπως πύλες (gateways), γέφυρες (bridges), δρομολογητές (routers), αναδιαμορφωτές (repeaters), κλπ. Σήμερα η έννοια διαδίκτυο περιλαμβάνει το μεγαλύτερο σύμπλεγμα διαφορετικών δικτύων

(net of nets) που χρησιμοποιούν ως πρωτόκολλο επικοινωνίας το TCP/IP, ενώ μπορεί να βρίσκονται εγκατεστημένα σε κάθε γωνιά του πλανήτη.

Το πρωτόκολλο TCP/IP (Transmission Control Protocol / Internet Protocol) είναι μια προ-συμφωνημένη μέθοδος επικοινωνίας και μεταφοράς δεδομένων στο Internet που χρησιμοποιείται κατά κανόνα. Βασίζεται στη λογική του «πακέτου», πράγμα που σημαίνει ότι στο κόμβο του αποστολέα το μήνυμα μετάδοσης «κόβεται» σε μικρότερα τμήματα ίδιου μεγέθους, τα οποία μεταδίδονται ανεξάρτητα μέσω του δικτύου. Κάθε πακέτο μεταφέρει ζωτικά στοιχεία για τη δρομολόγησή του (όπως π.χ. η διεύθυνση προορισμού του) και ακολουθεί τη δική του διαδρομή μέσα στο δίκτυο. Όταν τα πακέτα φτάσουν στο κόμβο του παραλήπτη, συναρμολογούνται για να σχηματιστεί το αρχικό μήνυμα. Φυσικά, η όλη διαδικασία προϋποθέτει ότι κάθε υπολογιστής στο διαδίκτυο έχει τη δική του διεύθυνση επικοινωνίας (IP address). Με τον τρόπο δημιουργήθηκαν κατανεμημένα δίκτυα (distributed networks) τα οποία δεν εξαρτώνται από ένα κέντρο οργάνωσης /ελέγχου και άρα δεν χρειάζεται να στηρίζουν τη λειτουργία τους σε κάποιο κεντρικό υπολογιστή.

2.3.4 **Δίκτυα ευρείας περιοχής**

Ένα δίκτυο ευρείας περιοχής (wide area network – WAN) χρησιμοποιείται για να καλύπτει μια μεγάλη γεωγραφική περιοχή, όπως π.χ. μια χωρά ή μια ήπειρος. Το δίκτυο αυτό περιλαμβάνει μια συλλογή από μηχανήματα που χρησιμοποιούνται για να τρέχουν τις διάφορες εφαρμογές των χρηστών. Στα περισσότερα δίκτυα WAN, το υποδίκτυο απαρτίζεται από δύο βασικά στοιχεία: τις γραμμές μετάδοσης και τα στοιχεία μεταγωγής. Οι γραμμές μετάδοσης είναι αυτές που μεταφέρουν τα bit μεταξύ των μηχανημάτων.

Τα στοιχεία μεταγωγής είναι εξειδικευμένοι υπολογιστές που συνδέουν δύο ή περισσότερες γραμμές μετάδοσης. Συγκεκριμένα, όταν τα δεδομένα φθάσουν σε μια εισερχόμενη γραμμή, τότε το στοιχείο μεταγωγής είναι αυτό που πρέπει να

επιλέξει μια εξερχόμενη γραμμή στην οποία να τα προωθήσει, γι' αυτό λέγονται και δρομολογητές. Το δίκτυο των περισσότερων WAN περιλαμβάνει πολλά καλώδια ή τηλεφωνικές γραμμές, καθένα από τα οποία συνδέει δύο δρομολογητές. Αν δύο δρομολογητές που δεν μοιράζονται ένα καλώδιο επιθυμούν να επικοινωνήσουν, πρέπει να το κάνουν εμμέσως, μέσω άλλων δρομολογητών. Όταν ένα πακέτο στέλνεται από έναν δρομολογητή σε άλλον μέσω ενός ή περισσοτέρων ενδιαμέσων δρομολογητών, το πακέτο παραλαμβάνεται ολόκληρο από κάθε ενδιάμεσο δρομολογητή, αποθηκεύεται εκεί μέχρι να ελευθερωθεί η απαιτούμενη εξερχόμενη γραμμή, οπότε και προωθείται.

3 ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ

Με το όρο ασφάλεια εννοούμε τη διαρκή και συνεχόμενη προστασία ενός αντικειμένου από τυχόν επιθέσεις. Το αντικείμενο αυτό θα μπορούσε να είναι ένα πρόσωπο, ένας οργανισμός, όπως μια επιχείρηση, ή κάποιο προσωπικό στοιχείο, όπως ένα υπολογιστικό σύστημα ή ένα αρχείο. Όταν αναφερόμαστε σε ένα υπολογιστικό σύστημα, η ασφάλειά του περιλαμβάνει την ασφάλεια όλων των στοιχείων του, όπως η CPU, η οθόνη, ο εκτυπωτής και άλλα. Επιπρόσθετα στα φυσικά στοιχεία του, θα πρέπει να προστατεύουν και τα μη-φυσικά στοιχεία του, όπως τα δεδομένα και η πληροφορία. Σε ένα διανεμημένο υπολογιστικό σύστημα, όπως είναι ένα δίκτυο, η προστασία καλύπτει τόσο τα φυσικά, όσο και τα μη-φυσικά στοιχεία του, στα οποία περιλαμβάνονται τα κανάλια επικοινωνίας και σύνδεσης (μόντεμ, γέφυρες, διακόπτες, servers) καθώς και τα αρχεία που είναι αποθηκευμένα σε αυτούς τους διακομιστές. Σε όλες τις περιπτώσεις, η ασφάλεια αντιστοιχεί στη παρεμπόδιση της μη εξουσιοδοτημένης πρόσβασης, χρήσης, αλλαγής και κλοπής ή καταστροφής αυτών των στοιχείων. Συνεπώς, ο όρος *ασφάλεια* περιλαμβάνει τις εξής έννοιες:

1. *Εμπιστευτικότητα*: για να παρεμποδιστεί η μη εξουσιοδοτημένη αποκάλυψη της πληροφορίας σε τρίτους.
2. *Ακεραιότητα*: για να παρεμποδιστεί η μη εξουσιοδοτημένη επεξεργασία των στοιχείων του δικτύου και να διατηρηθεί η κατάστασή του. Περιλαμβάνει την ακεραιότητα των στοιχείων του συστήματος, της πληροφορίας και του προσωπικού.
3. *Προσβασιμότητα*: για να παρεμποδιστεί η μη εξουσιοδοτημένη παρακράτηση των στοιχείων του συστήματος από αυτούς που τα χρειάζονται.

Βάσει των παραπάνω στοιχείων, η ασφάλεια διακρίνεται σε δύο είδη: τη φυσική ασφάλεια και την pseudo-ασφάλεια, που αναλύονται εκτενώς παρακάτω.

3.1 **Φυσική ασφάλεια**

Η φυσική ασφάλεια μπορεί να διασφαλιστεί εάν ισχύουν και εφαρμόζονται οι εξής τέσσερις μηχανισμοί: αναχαίτιση, πρόληψη, ανίχνευση και απόκριση.

- Η **αναχαίτιση** είναι συνήθως η πρώτη γραμμή άμυνας ενάντια στους εισβολείς που μπορεί να προσπαθήσουν να κερδίσουν πρόσβαση στο σύστημα. Ο τρόπος που λειτουργεί περιλαμβάνει τη δημιουργία μιας ατμόσφαιρας που σκοπό έχει να τρομοκρατήσει τους εισβολείς, όπως προειδοποιήσεις για σοβαρές συνέπειες αν αθετηθεί η ασφάλεια.
- Η **πρόληψη** είναι η διαδικασία κατά την οποία προσπαθούμε να σταματήσουμε τους εισβολείς να κερδίσουν πρόσβαση στους πόρους του συστήματος. Τα εμπόδια που μπορούμε να θέσουμε περιλαμβάνουν τα firewalls, DMZ και τη χρήση κλειδιών (keys), καρτών πρόσβασης, biometrics κτλ, ώστε να επιτρέπεται η πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες.
- Η **ανίχνευση** λαμβάνει χώρα όταν ένας εισβολέας έχει επιτύχει ή βρίσκεται στη διαδικασία ανάκτησης πρόσβασης στο σύστημα. Η διαδικασία ανίχνευσης περιλαμβάνει μηνύματα ειδοποίησης για την ύπαρξη εισβολέα. Τα μηνύματα αυτά μπορεί να είναι σε πραγματικό χρόνο ή να αποθηκεύονται για μελλοντική μελέτη.
- Η **απόκριση** είναι ένας μηχανισμός που ενεργοποιείται μετά την ειδοποίηση για εισβολή και με αυτό τον τρόπο γίνεται προσπάθεια ανταπόκρισης στην αστοχία των τριών προηγούμενων μηχανισμών. Ο τρόπος λειτουργίας βασίζεται στη προσπάθεια παύσης ή/και παρεμπόδισης μελλοντικής ζημιάς ή πρόσβασης σε μια υπηρεσία.

Εντός του συστήματος, η ασφάλεια επιτυγχάνεται και ενισχύεται με τη χρήση ηλεκτρονικών περιοριστικών μέτρων, όπως είναι τα firewalls και οι κωδικοί πρόσβασης (passwords).

3.1.1 Firewalls

Το firewall είναι ένα λογισμικό που χρησιμοποιείται για να απομονώσει μια ευαίσθητη περιοχή ενός συστήματος από τις διάφορες εξωτερικές επιρροές και να περιορίσει την πιθανή ζημιά που μπορεί να προκληθεί από κάποιον εισβολέα. Αν και δεν υπάρχει στάνταρ δομή ενός firewall, αφού εξαρτάται από το ίδιο το σύστημα και τις αναμενόμενες απειλές προς αυτό, εντούτοις τα περισσότερα firewalls είναι παραλλαγές κάποιων κοινών μοντέλων.

3.1.2 **Κωδικοί πρόσβασης**

Ένας κωδικός πρόσβασης είναι ένα αλφαριθμητικό που αποτελείται συνήθως από 6 έως 8 χαρακτήρες με διάφορους περιορισμούς στο μήκος και τον αρχικό χαρακτήρα, με σκοπό να επιβεβαιώσει την ταυτότητα του χρήστη, όταν αυτός θα προσπαθήσει να εισέλθει σε ένα υπολογιστικό σύστημα. Η ασφάλεια του κωδικού εξαρτάται σημαντικά από τους παρακάτω κανόνες:

- Να μην αποκαλύπτεται ποτέ ο κωδικός
- Να μην καταγράφεται ο κωδικός σε χαρτί
- Να μην επιλέγεται ένας κωδικός που θα είναι εύκολο να τον μαντέψει κάποιος
- Να αλλάζεται συχνά ο κωδικός

Συνεπώς γίνεται κατανοητό ότι η ασφάλεια του κωδικού πρόσβασης είναι σημαντική όχι μόνο για τους χρήστες των οποίων τα αρχεία είναι αποθηκευμένα στο σύστημα, αλλά είναι ζωτικής σημασίας και για το ίδιο το σύστημα, καθώς στη περίπτωση που ένας εισβολέας ανακτήσει πρόσβαση σε έναν κωδικό, τότε θα έχει

καταφέρει να εισχωρήσει στο σύστημα και έτσι όλα τα αρχεία και δεδομένα βρίσκονται εκτεθειμένα.

3.2 Pseudo-**ασφάλεια**

Η έννοια της ψευτο-ασφάλειας είναι η ασφάλεια μέσω της αφάνειας (securitythroughobscurity – STO), η οποία δίνει μια εσφαλμένη εντύπωση ασφάλειας. Δεν χρησιμοποιούνται προστατευτικοί τοίχοι, firewalls ή κωδικοί, ενώ η ασφάλεια εξαρτάται αποκλειστικά από τη φιλοσοφία ότι ο χρήστης δεν είναι επικίνδυνος για όσο διάστημα δεν έχει γνώσεις που θα μπορούσαν να επηρεάσουν την ασφάλεια του συστήματος, όπως π.χ. το δίκτυο.

4 ΣΤΟΧΟΙ ΑΣΦΑΛΕΙΑΣ

Όταν λέμε ότι ένα σύστημα ή ένας πόρος είναι ασφαλής, εννοούμε ότι είναι προστατευμένος από εσωτερική ή εξωτερική μη εξουσιοδοτημένη πρόσβαση. Η ασφάλεια, λοιπόν, ενός συστήματος και των πόρων του συμπεριλαμβάνει την ασφάλεια των απτών μερών του (hardware), καθώς και των μη απτών μερών του, όπως είναι η πληροφορία και τα δεδομένα του συστήματος.

4.1 Hardware

Η προστασία του υλικού ενός συστήματος περιλαμβάνει την προστασία:

- Των αντικειμένων των χρηστών, όπως το πληκτρολόγιο, το ποντίκι, την οθόνη αφής και άλλα.
- Των αντικειμένων του δικτύου, όπως τα firewalls, τα hubs, τους διακόπτες, τα routers και τις εξόδους διαφυγής, που είναι ευάλωτα στους hackers.
- Των καναλιών επικοινωνίας δικτύου, με σκοπό να αποτραπούν οι εισβολείς από το να παρακολουθήσουν τις δικτυακές επικοινωνίες.

4.2 Λογισμικό

Η προστασία του λογισμικού περιλαμβάνει την προστασία των λειτουργικών συστημάτων, των πρωτοκόλλων, των προγραμμάτων περιήγησης, των διαφόρων εφαρμογών και όλων των δεδομένων που βρίσκονται αποθηκευμένα σε αποθηκευτικούς δίσκους και βάσεις δεδομένων. Επίσης, περιλαμβάνει την προστασία λογισμικών με πελατειακή σχέση, όπως χαρτοφυλάκια επενδύσεων, οικονομικά δεδομένα, καταγραφές ακινήτων, εικόνες και άλλα προσωπικά αρχεία που βρίσκονται σε υπολογιστές μιας επιχείρησης ή μιας οικίας.

5 ΥΠΗΡΕΣΙΕΣ ΑΣΦΑΛΕΙΑΣ

Έχει ήδη οριστεί η έννοια της ασφάλειας ως η παρεμπόδιση της μη εξουσιοδοτημένης πρόσβασης στους πόρους ενός συστήματος. Η παρεμπόδιση αυτή επιτυγχάνεται μέσω μιας σειράς υπηρεσιών ασφάλειας, που περιλαμβάνουν τον έλεγχο πρόσβασης (accesscontrol), την πιστοποίηση (authentication), την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη μη αποκήρυξη (non-repudiation).

5.1 Έλεγχος πρόσβασης

Ο έλεγχος πρόσβασης είναι μια υπηρεσία, με την οποία, μαζί με τις υπόλοιπες πληροφορίες ταυτοποίησης του χρήστη (π.χ. κωδικός πρόσβασης) το σύστημα αποφασίζει ποιος χρήστης χρησιμοποιεί κάποια εφαρμογή του. Υπάρχουν συστήματα ελέγχου πρόσβασης που βασίζονται στο υλικό (hardware) και περιλαμβάνουν δακτυλικά αποτυπώματα, αναγνώριση φωνής και ματιού, οπτική παρακολούθηση με βίντεο, ηχητικά σήματα και τεχνολογίες GPS για εντοπισμό θέσης, κάρτες ταυτοποίησης.

Μια άλλη κατηγορία συστημάτων ελέγχου είναι αυτά που βασίζονται στο λογισμικό και διακρίνονται σε συστήματα με έλεγχο σημείου (Pointofaccess - POA) και απομακρυσμένου ελέγχου (Remotemonitoring). Στα συστήματα με έλεγχο σημείου οι δραστηριότητες του χρήστη παρακολουθούνται από έναν υπολογιστή που μπορεί να είναι συνδεδεμένος στο δίκτυο ή σε κάποιο ειδικό μηχάνημα και συλλέγονται και αποθηκεύονται οι προσπάθειες πρόσβασης σε ένα σύστημα. Στα συστήματα με απομακρυσμένο έλεγχο τα τερματικά μπορεί να συνδέονται μεταξύ τους με διάφορους τρόπους, όπως μόντεμ, τηλεφωνικές γραμμές και όλες τις μορφές ασύρματων συνδέσεων.

5.2 Πιστοποίηση

Η πιστοποίηση είναι ένας τρόπος για την ταυτοποίηση ενός χρήστη, η οποία μπορεί να είναι εξαιρετικά δύσκολη, ειδικά για έναν απομακρυσμένο χρήστη, καθώς πολλοί χρήστες και ειδικότερα αυτοί που προτίθενται να προκαλέσουν ζημιά σε ένα υπολογιστικό σύστημα, συνήθως μεταμφιέζονται. Με αυτή τη διαδικασία το σύστημα συγκεντρώνει πληροφορίες σχετικά με το χρήστη για να εξασφαλίσει ότι είναι αυθεντικός, ενώ όταν πρόκειται για επικοινωνία και ανταλλαγή δεδομένων, η πιστοποίηση χρησιμοποιείται για να ταυτοποιηθεί ο αποστολέας και η ακεραιότητα του μηνύματος. Στα υπολογιστικά συστήματα τα πρωτόκολλα πιστοποίησης που είναι βασισμένα στην κρυπτογράφηση χρησιμοποιούν μεθόδους secret-key ή public-key για να κρυπτογραφήσουν ένα μήνυμα, μια διαδικασία που ονομάζεται ψηφιακή υπογραφή.

Η πιστοποίηση των χρηστών βασίζεται στον έλεγχο των παρακάτω πραγμάτων:

- Όνομα χρήστη
- Κωδικό πρόσβασης
- Εικόνα του αμφιβληστροειδούς, η οποία καταγράφεται μέσω ενός ειδικού μηχανήματος που σαρώνει και αποτυπώνει την εικόνα του αμφιβληστροειδούς και την αποθηκεύει στο σύστημα για τον έλεγχο και τη σύγκριση
- Δακτυλικά αποτυπώματα
- Φυσική θέση
- Κάρτες ταυτότητας

5.3 Εμπιστευτικότητα

Για την προστασία των δεδομένων ενός συστήματος και των πληροφοριών του από μη εξουσιοδοτημένη αποκάλυψη χρησιμοποιείται η υπηρεσία της

εμπιστευτικότητας. Όταν τα δεδομένα φεύγουν από το ένα άκρο, που μπορεί να είναι ο client υπολογιστής ενός δικτύου, τότε βρίσκονται εκτεθειμένα σε ένα επικίνδυνο περιβάλλον. Για το λόγο αυτό, ο παραλήπτης ενός μηνύματος δεν θα πρέπει να εμπιστεύεται εξ' ολοκλήρου τα δεδομένα που λαμβάνει, καθώς μπορεί να έχει διεισδύσει κάποιος τρίτος σε αυτά. Με την υπηρεσία της εμπιστευτικότητας χρησιμοποιούνται αλγόριθμοι για να εξασφαλιστεί ότι δεν έχουν διαστρεβλωθεί τα δεδομένα.

5.4 **Ακεραιότητα**

Με την ακεραιότητα προστατεύονται τα δεδομένα ενάντια σε απειλές που πρόκειται να τα αλλάξουν, να τα σβήσουν ή να τα αλλοιώσουν με οποιονδήποτε τρόπο. Όπως συμβαίνει και με την εμπιστευτικότητα, όταν τα δεδομένα ταξιδεύουν ανάμεσα στον αποστολέα και τον παραλήπτη, είναι ευάλωτα σε πολλές απειλές από hackers και ειδικούς στις κρυπτογραφήσεις, οι οποίοι έχουν ως στόχο τα υποκλέψουν τα δεδομένα αυτά και να τα αλλοιώσουν βάσει των κινήτρων που έχουν.

5.5 **Μη αποκήρυξη**

Είναι ένας τρόπος για να αποδεικνύεται η προέλευση μιας πληροφορίας καθώς και η μεταφορά της. Με αυτόν τον τρόπο και χρησιμοποιώντας ψηφιακές υπογραφές και αλγόριθμους κρυπτογράφησης, εξασφαλίζεται ότι τα ψηφιακά δεδομένα δεν θα αποκηρυχτούν, καθώς παρέχονται αποδείξεις για την προέλευσή τους που είναι δύσκολο να αμφισβητηθούν.

6 ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑΣ

Λόγω του ότι οι διάφορες λύσεις για την ασφάλεια των συστημάτων χρησιμοποιούν διαφορετικούς τύπους και τεχνολογίες, έχουν δημιουργηθεί ορισμένα πρωτόκολλα ασφάλειας, έτσι ώστε να υπάρχει λειτουργικότητα και ομοιομορφία μεταξύ των πολλών συστημάτων και πόρων και των διαφόρων τεχνολογιών που υπάρχουν πίσω από αυτά. Εν ολίγης, το είδος του πρωτοκόλλου που εφαρμόζεται κάθε φορά εξαρτάται από τη φύση και το μέγεθος της επιχείρησης/οργανισμού που θα το εφαρμόσει. Παρακάτω θα αναλυθούν τα πρωτόκολλα ασφαλείας βάσει του τύπου του οργανισμού ή της επιχείρησης, του μεγέθους της και των ενδιαφερόντων της.

6.1 Πρωτόκολλα ασφαλείας βάσει του τύπου του οργανισμού/επιχείρησης

Πολλές φορές οι διοικήσεις ασφαλείας σε μια επιχείρηση επιλέγουν το είδος του πρωτοκόλλου που πρόκειται να εφαρμόζεται με βάση τον τύπο των υπηρεσιών που προσφέρει η επιχείρηση αυτή. Στον παρακάτω πίνακα 2 δίνονται μερικές από αυτές τις υπηρεσίες και τα αντίστοιχα πρωτόκολλα που μπορούν να εφαρμοστούν για αυτές, ενώ αμέσως μετά αναλύονται εκτενέστερα μερικά από αυτά.

Περιοχή εφαρμογής	Υπηρεσία	Πρωτόκολλο ασφάλειας
Ασφάλεια διαδικτύου	Πιστοποίηση δικτύου	Kerberos
	Ασφαλείς επικοινωνίες TCP/IP μέσω του διαδικτύου	IPSec
	Ηλεκτρονικό ταχυδρομείο	S/MIME, PGP
	Public key στάνταρ	3-DES, DSA, RSA, MD-5,

	κρυπτογράφησης	SHA-1, PKCS
	Πρωτόκολλο ασφαλούς μεταφοράς υπέρ-κειμένου (hypertext)	S-HTTP
	Πιστοποίηση χρηστών καταλόγου	X.509/ISO/IEC 9594-8:2000:
	Πρωτόκολλο ασφαλείας για ιδιωτικότητα στο διαδίκτυο και τη μεταφορά	SSL, TLS, SET
Ψηφιακή υπογραφή και κρυπτογράφηση	Στάνταρ κρυπτογράφησης/ PKI / ψηφιακά αποδεικτικά, XML ψηφιακές υπογραφές	X509, RSA BSAFE SecurXML-C, DES, AES, DSS/DSA, EESSI, ISO 9xxx, ISO, SHA/SHS, XML Digital Signatures, XML Encryption, XML Key Management Specification
Είσοδος και πιστοποίηση	Πιστοποίηση του δικαιώματος του χρήστη να χρησιμοποιήσει το σύστημα ή τους πόρους του δικτύου	SAML, Liberty Alliance, FIPS 112
Firewall **και ασφάλεια συστήματος**	Ασφάλεια τοπικών, ευρέων και μητροπολιτικών δικτύων	SDE πρωτόκολλο για IEEE 802, ISO/IEC 10164

Πίνακας 2. **Πρωτόκολλα ασφαλείας με βάση τις υπηρεσίες**

6.1.1 Public key **στανταρ κρυπτογράφησης** (PKCS)

Αυτά τα πρωτόκολλα ασφαλείας είναι σχετικά πρόσφατα, εκδόθηκαν για πρώτη φορά το 1991 και έκτοτε χρησιμοποιούνται ευρέως και αποτελούν τη βάση για πολλά άλλα στανταρ. Σε γενικές γραμμές, τα PKCS είναι χαρακτηριστικά ασφαλείας που παράχθηκαν από τα RSALaboratories με σκοπό την επιτάχυνση της public-key κρυπτογραφίας.

6.1.2 S/MIME

Το S/MIME (SecureMultipurposeInternetMailExtensions) είναι ένα χαρακτηριστικό για την ασφαλή αποστολή ηλεκτρονικών μηνυμάτων. Εμφανίστηκε όταν ήρθε στην επιφάνεια το ολοένα και αυξανόμενο πρόβλημα των υποκλοπών της ηλεκτρονικής αλληλογραφίας και πλαστογραφίας, λόγω της αύξουσας πορείας που είχαν πάρει οι ψηφιακές επικοινωνίες. Έτσι, το 1995 διάφοροι προμηθευτές λογισμικού δημιούργησαν το χαρακτηριστικό S/MIME, με αρχικό στόχο την εύκολη ασφάλιση των μηνυμάτων από τα «αδιάκριτα βλέμματα».

Η λειτουργία του επιτυγχάνεται μετά δημιουργία ενός στρώματος ασφαλείας πάνω από το βιομηχανικό πρωτόκολλα MIME, η οποία βασίζεται στο PKCS. Η χρήση του PKCS προδίδει στο χρήστη του S/MIME με άμεση ιδιωτικότητα, ακεραιότητα των δεδομένων του και πιστοποίηση ενός ηλεκτρονικού μηνύματος. Με αυτό τον τρόπο το συγκεκριμένο στανταρ έχει ευρεία αποδοχή, γεγονός που έχει οδηγήσει στο S/MIME να χρησιμοποιείται και πέραν των e-mails. Πολλές εταιρίες λογισμικού, όπως η Microsoft, Lotus, Banyan και άλλες on-line υπηρεσίες ηλεκτρονικού εμπορίου χρησιμοποιούν το S/MIME.

6.1.3 FIPS

Τα στάνταρ FIPS (FederalInformationProcessingStandards) είναι εγκεκριμένα στάνταρ από το Εθνικό Ινστιτούτο Πιστοποίησης και Τεχνολογίας (NationalInstituteofStandardsandTechnology – NIST) σχετικά με την προηγμένη κρυπτογράφηση. Η Αμερικανική κυβέρνηση προτείνει τη χρήση τους σε

κυβερνητικούς οργανισμούς και άλλους στον ιδιωτικό τομέα, ώστε να προστατεύονται οι ευαίσθητες πληροφορίες. Υπάρχουν διάφορες εκδόσεις που κυμαίνονται από το FIPS 31, που ιδρύθηκε το 1974 μέχρι το FIPS 198 που ισχύει σήμερα.

6.1.4 SecureSocketsLayer (SSL)

Το SSL είναι ένα στάνταρ κρυπτογράφησης που χρησιμοποιείται στις περισσότερες διαδικτυακές συναλλαγές, ενώ έχει μετατραπεί στον πιο δημοφιλή τρόπο κρυπτογράφησης των ηλεκτρονικών συναλλαγών. Παρέχει τα διάφορα στοιχεία της κρυπτογράφησης ενσωματωμένα μέσα στο πρωτόκολλο TCP/IP. Έχει αναπτυχθεί από την NetscapeCommunications και παρέχει ασφαλή επικοινωνίας μεταξύ client και server, συμπεριλαμβανομένης της κρυπτογράφησης, της πιστοποίησης και ακεραιότητας των δεδομένων όταν αναζητά μια TCP/IP σύνδεση.

6.2 Πρωτόκολλα ασφαλείας βάσει του μεγέθους/χρήσης του οργανισμού/επιχείρησης

Σε περίπτωση που το δίκτυο είναι μικρό ή πρόκειται για μικρή επιχείρηση, όπως ένα πανεπιστήμιο, τότε τα πρότυπα ασφαλείας μπορούν να διατυπώνονται ως η καλύτερη πρακτική σχετικά με την ασφάλεια του συστήματος, συμπεριλαμβανομένης της φυσικής ασφάλειας εξοπλισμού, λειτουργικών συστημάτων και λογισμικού εφαρμογών.

- Φυσική ασφάλεια – δίνει έμφαση στην ανάγκη για ασφάλεια των υπολογιστών που αποτελούν τους servers του διαδικτύου και το πώς αυτοί οι υπολογιστές μπορούν να διατηρηθούν ασφαλείς σε μια κλειδωμένη περιοχή. Επίσης, τα πρότυπα χρειάζονται για αποθηκευτικά μέσα, όπως δίσκοι.

- Λειτουργικά συστήματα – εδώ δίνεται έμφαση στα δικαιώματα και τον αριθμό των λογαριασμών, βάσει των οποίων ρυθμίζονται τα πρότυπα. Για παράδειγμα, ο αριθμός των χρηστών με την πιο προνομιακή πρόσβαση όπως το root στα UNIX ή το Administrator στα Windows θα πρέπει να είναι ελάχιστος. Επίσης, θα πρέπει να υπάρχουν όροι για τους προνομιούχους χρήστες, να διατηρείται ένας ελάχιστος αριθμός λογαριασμών χρηστών στο σύστημα, να διατηρείται ένας ελάχιστος αριθμός υπηρεσιών που προσφέρονται στους clientcomputers από το server και να υπάρχει ένα πρότυπο πιστοποίησης, όπως κωδικοί.
- Καταγραφές συστήματος. Οι καταγραφές περιέχουν πάντα ευαίσθητες πληροφορίες, όπως ημερομηνίες και ώρες πρόσβασης των χρηστών στο σύστημα. Αυτές οι πληροφορίες θα πρέπει να είναι προσβάσιμες μόνο σε εξουσιοδοτημένους χρήστες και όχι για το ευρύ κοινό.
- Ασφάλεια δεδομένων. Θα πρέπει να υπάρχει ένα πρότυπο για το χειρισμό των αρχείων που περιέχουν ευαίσθητα δεδομένα. Για παράδειγμα, αρχεία που περιέχουν σημαντικά δεδομένα θα πρέπει να κρυπτογραφούνται όποτε είναι δυνατόν ή να μεταφέρονται πολύ σύντομα σε ασφαλές σύστημα που δεν είναι προσβάσιμο από το ευρύ κοινό.

Ένα παράδειγμα για το πώς μπορεί να ρυθμιστούν τα πρότυπα ασφαλείας δίνεται στον παρακάτω πίνακα 3.

Περιοχή εφαρμογής	Πρότυπο ασφαλείας
Λειτουργικά συστήματα	Unix, Linux, Windows, etc.
Προστασία από ιούς	Norton
Email	PGP, S/MIME
Firewalls	

Telnet **και εφαρμογές** FTP terminal	SSH (secure shell)

Πίνακας3.

6.2 Πρωτόκολλα ασφαλείας βάσει των ενδιαφερόντων του οργανισμού/επιχείρησης

Σε πολλές περιπτώσεις οι οργανισμοί και οι κυβερνητικές οργανώσεις επιλέγουν να χρησιμοποιούν ένα πρότυπο ασφαλείας που να στηρίζεται αποκλειστικά στα ενδιαφέροντα του οργανισμού ή της χώρας. Στον παρακάτω πίνακα 4 δίνονται μερικά τέτοια πρότυπα ασφάλειας.

Περιοχή εφαρμογής	Υπηρεσία	Πρότυπο ασφάλειας
Τραπεζικές εφαρμογές	Ασφάλεια σε συστήματα πληροφορικής σε τράπεζες	ISO 8730, ISO 8732, ISO/TR 17944
Οικονομικές εφαρμογές	Ασφάλεια σε οικονομικές υπηρεσίες	ANSI X9.x, ANSI X9.xx

Πίνακας4.

7 ΣΤΟΙΧΕΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ

Η επιλογή ενός συστήματος ασφάλειας ή συνδυασμού αυτών για το δίκτυο μιας επιχείρησης ή ενός οργανισμού εξαρτάται από πολλούς παράγοντες και, φυσικά, δεν υπάρχει η τέλεια ασφάλεια ενός συστήματος. Συνεπώς, η χρήση του ενός ή του άλλου στοιχείου εξαρτάται αποκλειστικά από τις ανάγκες της επιχείρησης, στην οποία ανήκουν τα υπολογιστικά συστήματα ή το δίκτυο.

7.1 Η πολιτική ασφάλειας

Γενικά υπάρχουν πολλές απόψεις σχετικά με την αναγκαιότητα ύπαρξης ενός σχεδίου ασφαλείας, αν και θεωρείται απαραίτητο να υπάρχει σε μια επιχείρηση. Ένα σχέδιο ασφαλείας αρχικά δίνει έμφαση σε μια σειρά από παράγοντες που πρέπει να διασφαλιστούν, ξεκινώντας από την αναγνώριση όλων των κρίσιμων λειτουργιών σε ένα σύστημα που πρέπει να προστατευτούν. Στη συνέχεια, ορίζει τις προτεραιότητες στους πόρους του συστήματος και στις πληροφορίες που βρίσκονται εκεί αποθηκευμένες. Επιπλέον, με την πολιτική ασφαλείας καθορίζονται παράγοντες κινδύνου σε όλους αυτούς τους πόρους και, με βάσει αυτούς, καταστρώνονται τα μέτρα ασφαλείας που πρέπει να ληφθούν. Τέλος, ένα πλάνο ασφαλείας θα πρέπει να λάβει υπόψη του το ανθρώπινο δυναμικό που χρησιμοποιεί το σύστημα, χωρίζοντάς τους σε ομάδες, ενώ θα πρέπει να υπάρχει μια μορφή εκπαίδευσης της κάθε ομάδας πάνω στους τρόπους ασφάλειας.

7.2 Έλεγχος πρόσβασης (Accesscontrol)

Παραπάνω αναφέρθηκε η αναγκαιότητα ύπαρξης ενός συστήματος ελέγχου της πρόσβασης. Καθώς η πληροφορία γίνεται όλο και πιο πολύτιμη και ολοένα και περισσότεροι άνθρωποι μπαίνουν στον κόσμο του διαδικτύου, παρατηρείται

αύξηση των hackers, ακτιβιστών, κλεφτών και διαφόρων άλλων ανθρώπων που συνεχίζουν να συρρέουν το διαδίκτυο, ενώ η ασφάλεια και η προστασία της πληροφορίας που βασίζεται στα δίκτυα έχει γίνει ζωτικής σημασίας.

7.3 Ισχυροί αλγόριθμοι κρυπτογράφησης

Καθώς επεκτείνονται τα δίκτυα, το ποσοστό της πληροφορίας που αποθηκεύεται και διασχίζει τα υπολογιστικά συστήματα και δίκτυα αυξάνεται τόσο σε όγκο όσο και σε αξία. Εντούτοις, η ασφάλεια αυτής της πληροφορίας απειλείται συνεχώς από την ποιότητα και την προστασία των λογισμικών εφαρμογών που υπάρχουν στους υπολογιστές, καθώς και από τους πολλούς hackers που προσπαθούν να προσπελάσουν αύτη την πληροφορία. Η εκτεταμένη έρευνα πάνω σε αυτό το πεδίο έχει δείξει ότι υπάρχει ένας μεγάλος όγκος ευάλωτων στοιχείων στη δομή των δικτύων και σχετικά φτωχά πρωτόκολλα ασφαλείας. Οι hackers εκμεταλλεύονται τα bugs των λογισμικών, τα οποία μερικές φορές είναι εύκολο να διορθωθούν, και έτσι αφουγκράζονται και παρακολουθούν τα δεδομένα επικοινωνίας με αυξανόμενη ευκολία. Η ασφάλεια της πληροφορίας, επομένως, έγκειται στην εύρεση ισχυρών αλγόριθμων κρυπτογράφησης που θα εκδιωχτούν τους εισβολείς.

7.4 Τεχνικές πιστοποίησης

Ως γνωστόν, σήμερα ένα μεγάλο μέρος των αγορών πραγματοποιείται ηλεκτρονικά παγκοσμίως και οι χρήστες ζητούν και απαιτούν έμπιστους και ισχυρούς αλγόριθμους που να καθιστούν αυτές τις συναλλαγές ασφαλείς. Μερικές από τις τεχνικές ασφάλειας που χρησιμοποιούνται σήμερα περιλαμβάνουν τις παρακάτω:

- Kerberos à πρόκειται για ένα βασικό σύστημα διαχείρισης που πιστοποιεί άγνωστους εντολείς που θέλουν να επικοινωνήσουν μεταξύ τους. Αρμοδιότητα του συστήματος αυτού είναι να εγγυάται για τις ταυτότητες

των χρηστών, διατηρώντας μια βάση δεδομένων με αυτούς που συμμετέχουν, τις διεργασίες, τους servers, τους ανθρώπους, τα συστήματα και άλλες πληροφορίες.

- IPSec **à** παρέχει τη δυνατότητα διασφάλισης των δεδομένων σε ένα δίκτυο επικοινωνίας. Αυτό επιτυγχάνεται με την κρυπτογράφηση ή την πιστοποίησης όλης της κίνησης σε επίπεδο δικτυακού IP. Με αυτό τον τρόπο όλες οι δικτυακές εφαρμογές (client/server, e-mail, filetransfer και Webaccess) γίνονται ασφαλείς.
- SSL (SecureSocketsLayer) **à** πρόκειται για μια ευέλικτη γενικής χρήσης κρυπτογράφηση που λειτουργεί σε επίπεδο TCP/IP για να πιστοποιήσει το server και, προαιρετικά, τον client. Με αυτό τον τρόπο το SSL καταλήγει να έχει ένα μυστικό κλειδί που χρησιμοποιείται τόσο από τον server όσο και από τον client για την αποστολή κρυπτογραφημένων μηνυμάτων.
- S/Key **à** είναι ένα σύστημα με κωδικό (password) που βασίζεται σε μια μονόδρομη hashfunction. Κάθε κωδικός που χρησιμοποιείται στο σύστημα έχει ισχύ μόνο για μία πιστοποίηση. Λόγω αυτής της μιας-χρήσεως πολιτικής, οι κωδικοί δεν μπορούν να υποκλαπούν και μια σειρά ενός κωδικού δεν παρέχει πληροφορίες για μελλοντικούς κωδικούς.
- ANSIX9.9 **à** πρόκειται για ένα πρότυπο τραπεζικής των ΗΠΑ για την πιστοποίηση τραπεζικών και οικονομικών συναλλαγών.
- ISO 8730 **à** πρόκειται για ένα διεθνές σύστημα πιστοποίησης ισοδύναμο με το ANSIX9.9.
- IndirectOTP (one-timepassword) **à** πρόκειται για μια τεχνική πιστοποίησης που δημιουργεί και χρησιμοποιεί ένα κωδικό μιας χρήσης και μετά τον διαγράφει. Ο server αποθηκεύει ή δημιουργεί εκ νέου μια προ-αποφασισμένη λίστα με κωδικούς που μπορεί να χρησιμοποιήσει ο χρήστης. Η ασφάλεια ενός OTP συστήματος βασίζεται στην μη αντιστρεψιμότητα μιας ασφαλούς hashfunction.

7.5 Έλεγχος

Σκοπός του ελέγχου αυτού είναι να εντοπιστούν όσο περισσότερα προβλήματα γίνεται σε ένα σύστημα προτού τα βρουν οι εισβολείς. Η φιλοσοφία είναι όσο περισσότερο ελέγχεται ένα σύστημα, τόσο πιο δύσκολο είναι να δεχτεί επίθεση το δίκτυο. Υπάρχουν δύο τύποι ελέγχου: ο ενεργός και ο παθητικός. Ο ενεργός έλεγχος περιλαμβάνει την ενεργή αντιμετώπιση της παράνομης πρόσβασης και εισβολής, ενώ ο παθητικός έλεγχος είναι ένας μηχανισμός που δεν γίνεται σε πραγματικό χρόνο. Βασίζεται σε κάποιον που θα ελέγξει τις καταγραφές και θα δράσει ανάλογα με την πληροφορία που περιέχουν.

8 ΤΟ E-MAIL ΚΑΙ ΟΙ ΑΠΕΙΛΕΣ

Η επικοινωνία σε πραγματικό χρόνο ή σχεδόν σε πραγματικό χρόνο είναι ένα εξαιρετικά σημαντικό στοιχείο της σημερινής κοινωνίας, αλλά και βασικό συστατικό της αρμονικής λειτουργίας ενός οργανισμού ή μιας επιχείρησης. Τα δύο βασικά μέσα επικοινωνίας, το email και τα άμεσα μηνύματα (InstantMessaging – IM) έχουν γίνει στόχος για κάποιους με εγκληματικούς σκοπούς. Κάποια μέσα, όπως το phishing, οι φαρσέρ κτλ βρίσκουν συνεχώς όλο και πιο έξυπνους τρόπους για να ξεγελάσουν το χρήστη να κατεβάσει ένα κακοήθες αρχείο ή να κλικάρει πάνω σε μια URL διεύθυνση, η οποία θα φορτώσει ένα μέρος κακόβουλου λογισμικού στον υπολογιστή του χρήστη.

8.1 Η διαχείριση των E-mails

Ο οργανισμός OpenText (2005) έχει δημιουργήσει ένα πλαίσιο Διαχείρισης Email (EmailManagementFramework) με σκοπό την καθοδήγηση των εταιριών στο να διατηρούν τις απαιτήσεις των emails. Το πλαίσιο αυτό βασίζεται σε τρία επίπεδα:

- Την αποθήκευση
- Τη διαχείριση και,
- Τη συμμόρφωση

Η ικανότητα αποθήκευσης περιλαμβάνει την αυτόματη μεταφορά των email από τον server σε μια συσκευή αποθήκευσης που να μπορεί να διατηρήσει αποτελεσματικά περισσότερα email, ενώ παράλληλα δίνει τη δυνατότητα στους χρήστες να εντοπίζουν εύκολα τα μηνύματά τους.

Η ικανότητα διαχείρισης στηρίζει τη νόμιμη ανακάλυψη και τη «διαχείριση δομημένης διατήρησης" των emails του οργανισμού.

Η ικανότητα συμμόρφωσης βοηθά τους οργανισμούς να εκπληρώνουν ορισμένες προϋποθέσεις, όπως π.χ. αυτές που τίθενται από το Υπουργείο Υγείας των ΗΠΑ.

8.2 **Μελλοντικές τάσεις στα** Emails

Τα email αποτελούν ένα καλά εδραιωμένο εργαλείο επικοινωνίας και συνεργασίας σε όλα τα επίπεδα των εργαζομένων μιας επιχείρησης ή ενός οργανισμού. Λόγω της ευρείας χρήσης του, το email έχει αποτελέσει και αποτελεί στόχο για αναρίθμητες επιθέσεις, κατά τις οποίες αποστέλλονται spam, ή επιθέσεις με σκοπό την κλοπή πληροφοριών και άλλων πολύτιμων δεδομένων. Ενώ το ποσοστό των ανεπιθύμητων email και επιθέσεων είναι αρκετά υψηλό, η τεχνολογία μαζί με διάφορους άλλους παράγοντες διατίθενται να μετριάσουν τις κακόβουλες επιθέσεις.

Σήμερα, οι εταιρίες που προμηθεύουν λογισμικά έχουν αρχίσει να αναπτύσσουν προϊόντα σχεδιασμένα να καταπολεμούν την εξάπλωση των spamemails και των μηνυμάτων «ψαρέματος» (phishing). Για παράδειγμα, η Microsoft έχει αναπτύξει του SenderIDFramework, ένα πλαίσιο που πιστοποιεί αν ένα μήνυμα έχει όντως σταλεί από κάποιον server που είναι εξουσιοδοτημένος από τον ιδιοκτήτη του domain να στέλνει μηνύματα. Επιπλέον, το πρότυπο που ακολουθεί η Yahoo! λειτουργεί ως εξής:

- Το domain του αποστολέα δημοσιεύει ένα publickey στα DNS αρχεία του
- Ο mailserver του αποστολέα υπογράφει ψηφιακά και αποστέλλει το μήνυμα
- Ο mailserver του παραλήπτη παραλαμβάνει το publickey από τα αρχεία του DNS του αποστολέα, πιστοποιεί την ψηφιακή υπογραφή χρησιμοποιώντας το περιεχόμενο του μηνύματος και,
- Ο mailserver του παραλήπτη παραλαμβάνει το email στα εισερχόμενα μηνύματά του.

Η Microsoft έχει ολοκληρώσει μια πειραματική έκδοση ενός εργαλείου άμυνας ενάντια στα spamemails, που λέγεται SmartProof και τα βασικά του λειτουργικά χαρακτηριστικά είναι:

1. Ένα φίλτρο με δυνατότητα εκμάθησης από την υπολογιστή εμποδίζει τα εμφανή spam μηνύματα και τα κρατά σε καραντίνα ή τα πετάει. Το φίλτρο μεταφέρει στα εισερχόμενα του χρήστη οποιοδήποτε μήνυμα έχει σταλεί από κάποιον που να βρίσκεται στην επιτρεπόμενη λίστα του χρήστη.
2. Τα ύποπτα μηνύματα για spam ενεργοποιούν αυτόματες απαντήσεις που στέλνονται στους αποστολείς, προκαλώντας τους να αποδείξουν ότι δεν είναι spammers.
3. Οι αποστολείς μπορούν να απαντούν στις προκλήσεις αυτές, λύνοντας κάποιο είδος παζλ, που θα είναι εύκολο να λυθεί από έναν άνθρωπο, αλλά δύσκολο από μια μηχανή αυτόματης δημιουργίας spam μηνυμάτων.
4. Εναλλακτικά, οι αποστολείς μπορούν να διασφαλίσουν την παράδοση των μηνυμάτων τους πραγματοποιώντας μικρές πληρωμές με πιστωτική κάρτα. Τα χρήματα μπορούν να κατατεθούν στον παραλήπτη, στον πάροχο της δικτυακής σύνδεσης ή σε φιλανθρωπίες ή μπορεί να επιστραφούν ξανά στον αποστολέα, αν το μήνυμα αποδειχτεί ότι δεν είναι spam.

Επιπροσθέτως, η Microsoft έχει αναγνωρίσει και ταυτοποιήσει πάνω από 70 διαφορετικούς τύπους αρχείων που πιστεύεται ότι θα μπορούσαν να αποτελέσουν κίνδυνο αν εκτελεστούν. Σε αυτή τη λίστα επικινδυνότητας περιλαμβάνονται και τα παρακάτω αρχεία:

- .bat – Microsoft batch file
- .cmd – Command file για Windows NT
- .scr – Screen saver
- .vb – Visual Basic file
- .wsf – Windows script file

Στη συνέχεια, εφόσον το ηλεκτρονικό ταχυδρομείο πιθανότατα θα παραμείνει το βασικό μέσο επικοινωνίας και στο προσεχές μέλλον, οι προσπάθειες θα πρέπει να επικεντρωθούν σε περιοχές επικοινωνίας που είναι δύσκολο να ελεγχθούν, όπως τα μπλογκς των υπαλλήλων μιας επιχείρησης. Η IBMResearch δημιούργησε πρόσφατα ένα εργαλείο που λέγεται ActivityExplorer και στόχο έχει να συγκεντρώσει τα μηνύματα ηλεκτρονικού ταχυδρομείου, τις συγχρονισμένες επικοινωνίες, τις εικόνες, τα αρχεία, τους φακέλους και τις to-do λίστες, ενώ η MicrosoftResearch ανέπτυξε έναν τρόπο για να συνδυάζει email, αρχεία, ηλεκτρονικές σελίδες, ημερολογιακές καταχωρήσεις, to-do λίστες και άλλο υλικό σε ένα αρχείο που μπορεί να ανιχνευτεί.

Τέλος, σειρά έχει η εξέλιξη των εφαρμογών που έχουν μετατρέψει τα εισερχόμενα μηνύματα σε αποθήκες διαχείρισης της γνώσης, αφού εκεί υπάρχουν παλιές και νεότερες εκδόσεις αρχείων, παρουσιάσεων και σχεδίων μιας επιχείρησης.

8.3 Simple Mail Transfer Protocol (SMTP)

Το SMTP είναι ένα πρωτόκολλο που ευθύνεται για την μεταφορά ηλεκτρονικών μηνυμάτων με ασφάλεια και αποτελεσματικότητα. Από προεπιλογή το SMTP χρησιμοποιεί την TCP θύρα 25. Το πρωτόκολλο για τη μεταφορά μηνυμάτων χρησιμοποιεί τη θύρα 587. Οι συνδέσεις SMTP που είναι ασφαλισμένες με SSL, γνωστές ως SMTPS, χρησιμοποιούν τη θύρα 465. Το SMTP προέρχεται από δύο υλοποιήσεις που περιγράφηκαν το 1971: το MailBoxProtocol, του οποίου η εφαρμογή βρισκόταν σε διαμάχη, και το πρόγραμμα SNDMSG. Άλλες υλοποιήσεις περιλαμβάνουν το FTPMail και το MailProtocol κατά το 1973. Το SMTP άρχισε να χρησιμοποιείται ευρέως στις αρχές της δεκαετίας του 1980.

Ενώ οι ηλεκτρονικοί server ηλεκτρονικής αλληλογραφίας και άλλες πλατφόρμες μεταφοράς μηνυμάτων χρησιμοποιούν το πρωτόκολλο SMTP για την αποστολή και

την παραλαβή ηλεκτρονικών μηνυμάτων, οι εφαρμογές πελάτη αλληλογραφίας σε επίπεδο χρήστη τυπικά χρησιμοποιούν το SMTP μόνο για την αποστολή μηνυμάτων σε ένα mailserver για απάντηση. Για την παραλαβή μηνυμάτων οι εφαρμογές αυτές χρησιμοποιούν είτε το πρωτόκολλο POP3 ή το IMAP. Ενώ τα ιδιόκτητα συστήματα (όπως το MicrosoftExchange και το LotusNotes της IBM) και τα συστήματα webmail (όπως το Hotmail, Gmail και Yahoo! Mail) χρησιμοποιούν τα δικά τους μη-τυποποιημένα πρωτόκολλα για να έχουν πρόσβαση στους λογαριασμούς εισερχομένων των δικών τους servers, παρόλα αυτά όλοι χρησιμοποιούν το πρωτόκολλο SMTP όταν στέλνουν ή παραλαμβάνουν ένα email από κάποιο εξωτερικό σύστημα από το δικό τους.

Το SMTP είναι ένα πρωτόκολλο κειμένου προσανατολισμένο στην εκάστοτε σύνδεση, στο οποίο ο αποστολέας του email επικοινωνεί με τον παραλήπτη εισάγοντας εντολές σε μορφή αλφαριθμητικών και παρέχοντας τα απαραίτητα δεδομένα μέσω ενός έμπιστου καναλιού μεταφοράς δεδομένων, δηλαδή μιας σύνδεσης TransmissionControlProtocol (TCP).

Το SMTP είναι αποκλειστικά ένα πρωτόκολλο αποστολής μηνυμάτων. Σε κανονική χρήση, το μήνυμα, όταν φτάνει, προωθείται σε έναν mailserver-προορισμό. Το μήνυμα αυτό κατευθύνεται ανάλογα με τον διακομιστή που προορίζεται και όχι βάσει του χρήστη για τον οποίο απευθύνεται. Άλλα πρωτόκολλα, όπως το PostOfficeProtocol (POP) και το InternetMessageAccessProtocol (IMAP) είναι ειδικά σχεδιασμένα για χρήση από ατομικούς χρήστες, οι οποίοι ανακτούν τα μηνύματά τους και διαχειρίζονται τα εισερχόμενα.

8.4 **Πρωτόκολλα ηλεκτρονικής αλληλογραφίας**

Τα πρωτόκολλα των email αφορούν κάποιες στάνταρ μεθόδους που χρησιμοποιούνται σε κάθε κανάλι επικοινωνίας με αποτέλεσμα να μεταφέρεται

κατάλληλα η πληροφορία. Προκειμένου να γίνει η διαχείριση των ηλεκτρονικών μηνυμάτων, θα πρέπει να χρησιμοποιείται ένας mailclient που θα έχει πρόσβαση στον mailserver και θα πρέπει να ανταλλάσσουν πληροφορίες μεταξύ τους χρησιμοποιώντας μια σειρά από πρωτόκολλα. Μερικά από αυτά αναλύονται παρακάτω.

8.4.1 **Πρωτόκολλο** IMAP

Το IMAP (InternetMessageAccessProtocol) είναι ένα στάνταρ πρωτόκολλο για πρόσβαση στα email από τον τοπικό διακομιστή. Πρόκειται για ένα πρωτόκολλο πελάτη/ διακομιστή (client/server), στο οποίο όταν λαμβάνεται ένα email, τότε αυτό αποθηκεύεται στον server του διαδικτύου. Λόγω του ότι η διαδικασία αυτή απαιτεί μόνο ένα μικρό μέγεθος δεδομένων που πρόκειται να μεταφερθούν, λειτουργεί εξίσου καλά ακόμα και για πιο αργές συνδέσεις, όπως με ένα απλό μόντεμ. Το μήνυμα «κατεβαίνει» από τον server μόνο στην περίπτωση που ο χρήστης ζητήσει να διαβάσει το περιεχόμενο ενός συγκεκριμένου μηνύματος. Με το πρωτόκολλο αυτό ο χρήστης μπορεί να δημιουργήσει και να χειριστεί φακέλους, να διαγράψει μηνύματα κτλ.

8.4.2 **Πρωτόκολλο POP**3

Το πρωτόκολλο POP3 (PostOfficeProtocol 3) παρέχει στους χρήστες έναν απλό και τυποποιημένο τρόπο για να αποκτούν πρόσβαση στο ηλεκτρονικό τους ταχυδρομείο και να κατεβάζουν μηνύματα στον υπολογιστή τους.

Όταν χρησιμοποιείται το πρωτόκολλο POP3 όλα τα emails «κατεβαίνουν» από τον διακομιστή των mails στον τοπικό υπολογιστή του χρήστη. Υπάρχει η δυνατότητα να αφήνονται αντίγραφα των μηνυμάτων στον διακομιστή. Το πλεονέκτημα σε αυτό είναι ότι εφόσον έχουν κατεβεί όλα τα μηνύματα, μπορεί να διακοπεί για οποιοδήποτε λόγο η σύνδεση στο Internet και παράλληλα να διαβαστούν όλα τα emails, χωρίς να απαιτείται η σύνδεση πια. Από την άλλη μεριά, με αυτή τη

διαδικασία μπορεί να έχουν κατέβει και πολλά ανεπιθύμητα μηνύματα (συμπεριλαμβανομένων των spam μηνυμάτων ή ιών).

8.4.3 **Πρωτόκολλο** SMTP

Το πρωτόκολλο SMTP (SimpleMailTransferProtocol) χρησιμοποιείται από το MailTransferAgent (MTA) για να παραδώσει τα μηνύματα στο διακομιστή των παραληπτών. Το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί μόνο για να στείλει emails και όχι για να παραλάβει. Ανάλογα με τις ρυθμίσεις του δικτύου/ISP, το SMTP ενδέχεται να μπορεί να χρησιμοποιηθεί μόνο υπό συγκεκριμένες συνθήκες.

8.4.4 **Πρωτόκολλο HTTP**

Το πρωτόκολλο HTTP δεν είναι αμιγώς προσανατολισμένο στις επικοινωνίες με ηλεκτρονικό ταχυδρομείο, αλλά μπορεί να χρησιμοποιηθεί για την πρόσβαση στο γραμματοκιβώτιο του χρήστη. Το πρωτόκολλο αυτό μπορεί να χρησιμοποιηθεί για τη σύνθεση ή ανάκτηση των emails από έναν λογαριασμό. Το Hotmail είναι ένα παράδειγμα χρήσης του πρωτοκόλλου HTTP ως πρωτόκολλο αλληλογραφίας.

8. 5 IBMLotusNotes

Το LotusNotes της IBM είναι μια πλατφόρμα διακομιστή-πελάτη που μπορεί να χρησιμοποιηθεί ως πλατφόρμα ηλεκτρονικής αλληλογραφίας με τον ίδιο τρόπο όπως ένα IMAP client. Παρέχει στους χρήστες ενσωματωμένες δυνατότητες ηλεκτρονικής αλληλογραφίας, ημερολογίου, άμεσων μηνυμάτων (instantmessaging), συζητήσεων και forum, blogs, ενώ δίνεται η δυνατότητα στους χρήστες να πραγματοποιούν τηλεδιασκέψεις ή video-κλήσεις, γεγονός που συμβάλει στην αύξηση της παραγωγικότητας των υπαλλήλων μιας επιχείρησης.

Το LotusNotes αποτελεί το πρώτο λογισμικό που υιοθετήθηκε ευρέως και χρησιμοποιεί κρυπτογραφία με publickey για πιστοποίηση client-server και server-server και για την κρυπτογράφηση των δεδομένων. Σύμφωνα με τους ισχύοντες

νόμους εξαγωγής των Ηνωμένων Πολιτειών, το IBMNotes υποστηρίζει μόνο μία έκδοση του NotesPKI με 128-bit συμμετρικών κλειδιών, 1024-bitpublickeys και κανένα workloadreductionfactor. Περιλαμβάνει εργαλεία ασφαλείας S/MIME, SSL 3.0 και άλλα πρωτόκολλα επικοινωνίας για το διαδίκτυο και πιστοποιητικά πελάτη X.509.

8.6 MicrosoftExchange

Ο διακομιστής MicrosoftExchange είναι ένα λογισμικό που περιλαμβάνει ημερολόγιο, διακομιστή ηλεκτρονικών μηνυμάτων και διαχειριστή επαφών που αναπτύχθηκε από τη Microsoft. Αρχικά η Microsoft ξεκίνησε το σχεδιασμό του Exchange 4.0 τον Απρίλιο του 1993 και τον Ιανουάριο του 1995 ο ExchangeBeta 1 χρησιμοποιούταν από 500 χρήστες. Τελικά, τον Απρίλιο του 1996 αριθμούσε 32000 νέους χρήστες.

Το 1997 κυκλοφόρησε το Exchange 5.0, που αποτελούσε την πιο ολοκληρωμένη λύση, καθώς έδινε τη δυνατότητα της εγκατάστασης server τοπικά και παρείχε επικοινωνία μέσω SMTP στα δίκτυα. Οι εκδόσεις αυτές είχαν αρκετούς περιορισμούς στη χρήση, όπως το μέγεθος των βάσεων δεδομένων που δεν μπορούσαν να ξεπερνάνε τα 16GB, πράγμα που ήταν περιοριστικό για τους χρήστες.

Αυτοί οι περιορισμοί ξεπεράστηκαν με το Exchange 6.0 αρχικά (Νοέμβριος 2000) και αργότερα με το Exchange 6.5 ή 2003, το οποίο είχε μεγαλύτερες απαιτήσεις σε υπολογιστικό σύστημα, υποστηρίζει βάσεις δεδομένων μέχρι 100GB, γεγονός που σήμαινε μεγαλύτερο αριθμό χρηστών, και μπορούσε να εγκατασταθεί μόνο σε συστήματα με λειτουργικό Windows 2000 Server με SP4 ή WindowsServer 2003. Η έκδοση αυτή έδινε τη δυνατότητα στο σύστημα να μπορεί να τίθεται γρηγορότερα online και παρείχε τη δυνατότητα του συγχρονισμού με διάφορες φορητές συσκευές. Είχε επίσης καλύτερη προστασία από ιούς και spam και έδινε τη δυνατότητα στον χρήστη να φιλτράρει τα εισερχόμενα email μέσω της IP του

αποστολέα. Η έκδοση αυτή ήταν προσανατολισμένη στη σχεδιαστή του MicrosoftOffice 2003, πράγμα που σημαίνει ότι οι χρήστες είχαν ένα κοινό περιβάλλον εργασίας.

9**ΑΜΕΣΑΜΗΝΥΜΑΤΑ** (INSTANT MESSAGING – **IM**)

Τα άμεσα μηνύματα ήρθαν σχετικά πρόσφατα στο προσκήνιο, ενώ στην αρχή τα χρησιμοποιούσαν περισσότερο οι έφηβοι για να διατηρούν επαφή με φίλους, πριν την άνοδο των κινητών τηλεφώνων. Με την πάροδο του χρόνου, όμως, το IM εξελίχθηκε σε ένα χρήσιμο εργαλείο και πλέον είναι κοινή πρακτική να κάνεις "chat" με πολλούς διαφορετικούς ανθρώπους ταυτόχρονα. Σε μια επιχείρηση, όπου απαιτείται η γρήγορη πληροφόρηση και κρίση των πραγμάτων, το IM αποδείχτηκε σωτήριο. Το βασικό μειονέκτημά του είναι ότι, λόγω της άτυπης μορφής επικοινωνίας, οι χρήστες/υπάλληλοι μιας επιχείρησης μπορεί να «ξεχαστούν» και να ανταλλάξουν σημαντικές πληροφορίες μέσω του chat. Ορισμένες επιχειρήσεις έχουν απαγορέψει τη χρήση του εν ώρα εργασίας, αλλά υπάρχουν και τρόποι ελέγχου, όπως η τυχαία παρακολούθηση κάποιων υπολογιστών με IM.

9.1 **Οι απειλές του IM**

Λόγω της ραγδαίας εξάπλωσης του IM και της δημοτικότητάς του, αποτελεί παράλληλα και έναν πολύ καλό στόχο για επιθέσεις των hackers. Το σκουλήκι (worm) αποτελεί την πιο συχνή επίθεση, καθώς είναι πολύ ανθεκτικά στο να ανιχνεύονται από τα παραδοσιακά λογισμικά, πράγμα που επιδεινώνεται από το γεγονός ότι συχνά μεταλλάσσονται, καθώς τα παραδοσιακά anti-virus λογισμικά αντιδρούν μόνο όταν εντοπίσουν ήδη καταγεγραμμένες επιθέσεις. Επιπλέον, το IM είναι ένας αγωγός για την ταχεία διάδοση των επιθέσεων μέσω της λίστας επαφών του χρήστη. Ακόμη πιο ανησυχητικό είναι ότι οι απειλές είναι σε θέση να κάνουν τη μετάβαση σε δίκτυα, καθώς και από τα δημόσια δίκτυα στα εσωτερικά. Παρακάτω παρατίθενται πέντε κίνδυνοι που έχουν εντοπιστεί σχετικά με την ασφάλεια των άμεσων μηνυμάτων.

- Η ταχεία υιοθέτηση και τη βελτίωση της λειτουργικότητας πρόκειται να οδηγήσουν σε ένα συνεχώς αυξανόμενο αριθμό των απειλών στο IM, οι οποίες αυξήθηκαν σχεδόν κατά 1700% το 2005, και δεδομένου ότι αναμένεται να υπάρχουν όλο και περισσότεροι χρήστες, δεν υπάρχει καμία ένδειξη ότι οι κίνδυνοι θα μειωθούν.
- Τα άμεσα μηνύματα περνούν από το αυστηρό μέσο ανταλλαγής γραπτών μηνυμάτων σε ένα μέσο που υποστηρίζει το πρωτόκολλο φωνής (VoiceOverInternetProtocolVOIP), καθώς και την τηλεδιάσκεψη. Καθώς η φωνή και το chatting ενσωματώνονται, αυτό θα δημιουργήσει μονοπάτια διαφυγής για καινούριες επιθέσεις σε πιθανούς στόχους.
- Τα σκουλήκια γίνονται όλο και πιο εξελιγμένα.
- Όσοι εκτελούν επιθέσεις θα συνεχίσουν να βλέπουν το IM σαν ένα καλό στόχο, αφού αποτελεί ένα πολύ καλό μέσο για την εξάπλωση των κακόβουλων επιθέσεων. Η αποστολή spam μέσω του IM γίνεται όλο και πιο συχνή, καθώς είναι πλέον εύκολη δουλειά να «ξεγελαστεί» ένας οργανισμός και να ξεκινήσει το «ψάρεμα» (phishing) πληροφοριών και δεδομένων.
- Τέλος, μέσω των άμεσων μηνυμάτων, μπορούν να χαθούν σημαντικά δεδομένα, όταν αποστέλλονται και μεταφέρονται αρχεία μέσω IM, μιας και δεν υπάρχει όριο στο μέγεθος των αρχείων που μπορούν να μεταφερθούν, όπως υπάρχει στην αποστολή email. Συνήθως δεν υπάρχουν φίλτρα περιεχομένου, συνεπώς δεν μπορούν να ελεγχθούν τα αρχεία που μεταφέρονται.

9.2 Πολιτικές προστασίας των άμεσων μηνυμάτων

Υπάρχουν τέσσερα σημεία που συνιστώνται για την προστασία των άμεσων μηνυμάτων ενός οργανισμού ή μιας επιχείρησης.

1. Αρχικά θα πρέπει να καθοριστούν τα όρια χρήσης του IM μέσα στην επιχείρηση. Η επικοινωνία με άμεσα μηνύματα είναι ακόμα μια αρκετά νέα τεχνολογία και οι περισσότερες επιχειρήσεις δεν έχουν αντιληφθεί ακόμα τον αντίκτυπο που θα έχει μια ανεξέλεγκτη χρήση του. Ένας έλεγχος χρήσης (Auditing) θα δείξει ποιος χρησιμοποιεί το IM και με ποιον επικοινωνεί.
2. Θα πρέπει να αναπτυχθεί μια στρατηγική για την προστασία της επιχείρησης από συγκεκριμένες απειλές προς IM. Όπως είναι λογικό, αρχικά θα πρέπει να ταυτοποιηθούν και να υπάρξει προστασία από τις πιο σημαντικές απειλές. Στη συνέχεια, θα πρέπει να αντιμετωπιστεί το ρίσκο για μελλοντικές επιθέσεις όπως επίσης η αμυντική γραμμή της επιχείρησης να παραμένει σε επαγρύπνηση, έτσι ώστε να μπορεί να εκτιμήσει αν το επίπεδο της άμυνάς της λειτουργεί σωστά και για τις παλιότερες επιθέσεις.
3. Θα χρειαστεί να αναπτυχθεί και να υλοποιηθεί μια πολιτική κωδικοποίησης της αποδεκτής χρήσης των άμεσων μηνυμάτων. Οι χρήστες-υπάλληλοι της εταιρίας θα πρέπει να εκπαιδευτούν στο να αντιλαμβάνονται την αποδεκτή και μη-αποδεκτή χρήση των IM σύμφωνα με τους κανόνες της επιχείρησης και η πολιτική της θα πρέπει να εξασφαλίζει ότι αυτό εφαρμόζεται.
4. Αφού δημιουργηθεί η πολιτική που περιγράφεται στο παραπάνω σημείο, το επόμενο στάδιο θα είναι να καθοριστεί η βέλτιστη κατεύθυνση για μια μακράς διαρκείας χρήση του IM μέσα στην επιχείρηση, καθώς με τη συνεχή εξέλιξη της τεχνολογίας των άμεσων μηνυμάτων, η χρήση τους θα πρέπει να παρακολουθείται επισταμένα.

10ΚΡΥΠΤΟΓΡΑΦΙΑ

Η αύξηση της χρήσης των υπολογιστών και των συστημάτων επικοινωνίας κατά τη δεκαετία του 1960 κατέστησε υπαρκτή την ανάγκη του ιδιωτικού τομέα να βρει τρόπους προστασίας της ψηφιακής πληροφορίας και να παρέχει υπηρεσίες ασφάλειας. Το πρότυπο κρυπτογράφησης δεδομένων (DataEncryptionStandard – DES), ξεκινώντας από τον Feistel στην IBM στις αρχές του ’70 και με αποκορύφωμα το 1977 με την υιοθέτησή του από το Αμερικανικό πρότυπο για την κρυπτογράφηση μη-ταξινομημένης πληροφορίας, αποτελεί τον πιο διαδεδομένο μηχανισμό κρυπτογράφησης στην ιστορία, ενώ παραμένει ο στάνταρ τρόπος διασφάλισης της ηλεκτρονικής εμπορικής για πολλούς οικονομικούς οργανισμούς ανά τον κόσμο.

Η πιο μεγάλη εξέλιξη στην ιστορία της κρυπτογραφίας έγινε το 1976, όταν οι Diffieκαι Hellman εξέδωσαν την εργασία *NewDirectionsinCryptography*, όπου εισάγεται η επαναστατική ιδέα της ασύμμετρης κρυπτογραφίας (public-keycryptography) και παράλληλα δίνονται νέες μέθοδοι για την ανταλλαγή κλειδιών. Αν και τότε οι συγγραφείς δεν είχαν πρακτική γνώση της ασύμμετρης κρυπτογραφίας, εντούτοις η ιδέα τους ήταν ξεκάθαρη και δημιούργησε ιδιαίτερη δραστηριότητα στο χώρο της κρυπτογραφίας. Το 1978 οι Rivest, Shamirκαι Adleman ανακάλυψαν τον πρώτο συνδυασμό ασύμμετρης κρυπτογράφησης και υπογραφής, που σήμερα αναφέρεται ως RSA και βασίζεται σε ένα δύσκολο μαθηματικό πρόβλημα. Μια από τις πιο σημαντικές συνεισφορές της public-key κρυπτογράφησης είναι η ψηφιακή υπογραφή, όπου το 1991 υιοθετήθηκε το πρώτο διεθνές πρότυπο για τις ψηφιακές υπογραφές (ISO/IEC 9796), που βασίζεται στο σύστημα RSA.

10.1 **Η ασφάλεια της πληροφορίας και η κρυπτογραφία**

Η ασφάλεια της πληροφορίας μπορεί να είναι αναγκαία σε πολλές καταστάσεις, αλλά στην περίπτωση των επικοινωνιών, όταν γίνεται μια συναλλαγή, τότε οι εμπλεκόμενοι σε αυτή θα πρέπει είναι πεπεισμένοι ότι ισχύουν συγκριμένες πτυχές της ασφάλειας της πληροφορίας. Μερικές από αυτές συνοψίζονται στον παρακάτω πίνακα 5.

Για να επιτευχθεί η ασφάλεια της πληροφορίας, όταν αυτή μεταφέρεται με ηλεκτρονικό τρόπο, τότε απαιτούνται πολλές τεχνικές γνώσεις και δεξιότητες. Παρόλα αυτά, δεν υπάρχει εγγύηση ότι θα επιτευχθεί η ασφάλεια στο μέγιστο. Η τεχνική μέθοδος που χρησιμοποιείται για να παρέχει ασφάλεια λέγεται κρυπτογραφία.

Η *κρυπτογραφία* είναι η μελέτη μαθηματικών τεχνικών που σχετίζονται με διάφορες πτυχές της ασφάλειας της πληροφορίας, όπως είναι η εμπιστευτικότητα, η ακεραιότητα των δεδομένων, η πιστοποίηση των οντοτήτων και η πιστοποίηση της προέλευσης των δεδομένων. Η κρυπτογράφηση δεν είναι ο μόνος τρόπος για την ασφάλεια των πληροφοριών. Οι αντικειμενικοί στόχοι της κρυπτογραφίας παρατίθενται στον πίνακα 5, ενώ παρακάτω δίνεται ένα πλαίσιο μέσα στο οποίο πρέπει να κινούνται οι στόχοι αυτοί.

1. Η *εμπιστευτικότητα* είναι μια υπηρεσία που χρησιμοποιείται για να διατηρείται μυστικό το περιεχόμενο της πληροφορίας από όλους, εκτός από αυτούς που είναι εξουσιοδοτημένοι. Υπάρχουν πολλοί τρόποι για να παρέχουμε εμπιστευτικότητα, είτε με φυσική προστασία ή με μαθηματικούς αλγόριθμους που καθιστούν τα δεδομένα απροσπέλαστα.
2. Η *ακεραιότητα των δεδομένων* είναι μια υπηρεσία που επισημαίνει την μη-εξουσιοδοτημένη αλλοίωση των δεδομένων. Για να εξασφαλιστεί η ακεραιότητα της πληροφορίας, θα πρέπει ο χρήστης να έχει τη δυνατότητα να εντοπίσει το χειρισμό των δεδομένων από μη εξουσιοδοτημένους χρήστες.

Ο χειρισμός αυτός μπορεί να περιλαμβάνει την εισαγωγή, τη διαγραφή και την αντικατάσταση πληροφοριών.

3. Η *πιστοποίηση* είναι μια υπηρεσία που σχετίζεται με την ταυτοποίηση και εφαρμόζεται τόσο στις οντότητες όσο και στην ίδια την πληροφορία. Όταν δύο μέρη (ή χρήστες) βρίσκονται εν μέσω μιας μορφής επικοινωνίας, θα πρέπει να ταυτοποιήσει ο ένας τον άλλον. Όταν διακινούνται πληροφορίες μέσω ενός καναλιού, τότε θα πρέπει να πιστοποιούνται όσον αφορά στην προέλευσή των δεδομένων, στο περιεχόμενό τους, την ώρα αποστολής τους κτλ. Για το λόγο αυτό, αυτή η πτυχή της κρυπτογραφίας συχνά διαχωρίζεται σε δύο βασικές κατηγορίες: την πιστοποίηση των οντοτήτων και την πιστοποίηση της προέλευσης. Η πιστοποίηση της προέλευσης των δεδομένων παρέχει ακεραιότητα των δεδομένων, καθώς π.χ. αν ένα μήνυμα έχει μεταβληθεί, τότε θα έχει μεταβληθεί και η πηγή αποστολής του.
4. Η *μη άρνηση αναγνώρισης* είναι μια υπηρεσία με την οποία μια οντότητα εμποδίζεται από το να αρνηθεί προηγούμενες δεσμεύσεις ή πράξεις. Όταν μια οντότητα αρνείται να δεχτεί ότι έχουν ληφθεί κάποια μέτρα και υπάρχει διαμάχη, τότε απαιτείται ένας τρόπος να επιλυθεί η κατάσταση. Για παράδειγμα, μια οντότητα μπορεί να δώσει έγκριση για την αγορά ενός αντικειμένου από μια άλλη οντότητα και αργότερα να αρνηθεί ότι δόθηκε μια τέτοια έγκριση. Μια τέτοια διαμάχη λύνεται όταν εμπλακεί μια τρίτη έμπιστη οντότητα.

Ιδιωτικότητα ή εμπιστευτικότητα	**Η διατήρηση της μυστικότητας των πληροφοριών από όλους εκτός από τους χρήστες που είναι εξουσιοδοτημένοι να τις δουν.**
Ακεραιότητα των δεδομένων	Η διασφάλιση ότι η πληροφορία δεν έχε

	αλλοιωθεί με μη-εξουσιοδοτημένου ή άγνωστους τρόπους.
Πιστοποίηση ή ταυτοποίηση των οντοτήτων	Επιβεβαίωση της ταυτότητας μιας οντότητας (π.χ. ενός προσώπου, ενός τερματικού υπολογιστή, μιας πιστωτικής κάρτας κτλ.)
Πιστοποίηση ενός μηνύματος	Επιβεβαίωση της πηγής μιας πληροφορίας, γνωστή και ως πιστοποίηση της προέλευσης της πληροφορίας
Υπογραφή	Ένας τρόπος να δεσμευτεί η πληροφορία σε μια οντότητα
Εξουσιοδότηση	Μεταφορά της επίσημης κύρωσης σε μια άλλη οντότητα να κάνει κάτι ή να είναι κάτι άλλο
Επικύρωση	Ένας τρόπος για να παρέχεται επικαιρότητα της άδειας χρήσης ή διαχείρισης της πληροφορίας
Έλεγχος πρόσβασης	Περιορισμός της πρόσβασης σε εξουσιοδοτημένες οντότητες
Πιστοποίηση	Επικύρωση των πληροφοριών από έναν αξιόπιστο φορέα
Timestamping	Καταγραφή της ώρας δημιουργίας ή ύπαρξης μιας πληροφορίας
Μαρτυρία	Επιβεβαίωση της δημιουργίας ή ύπαρξης μιας πληροφορίας από μια άλλη οντότητα πέραν του δημιουργού
Απόδειξη	Απόδειξη ότι η πληροφορία έχει

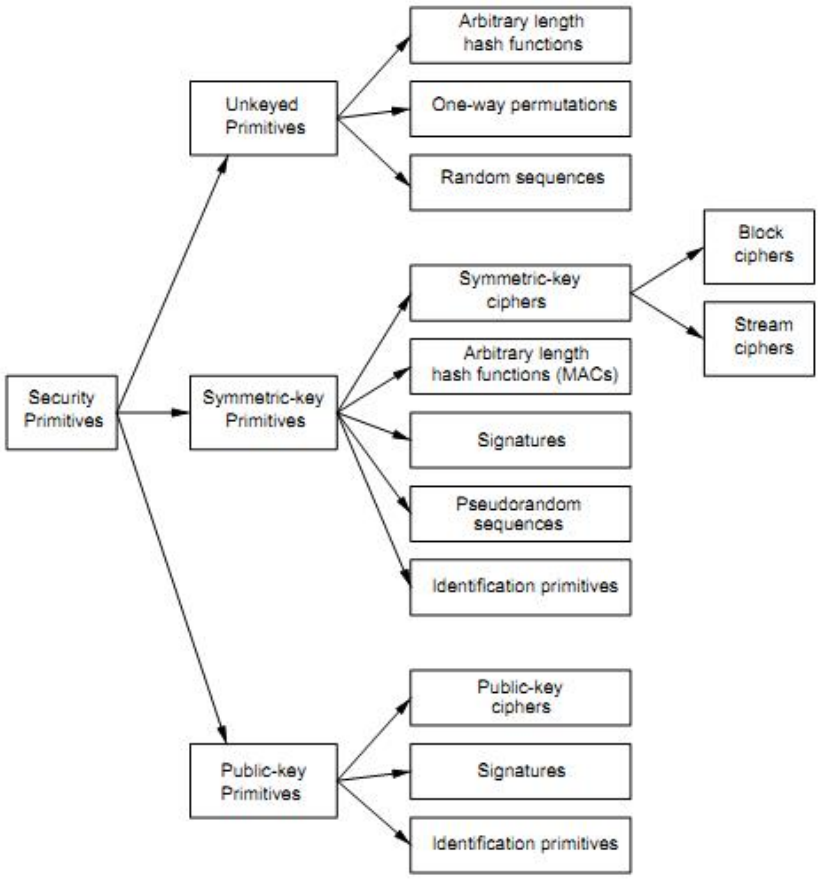
	παραληφθεί
Ιδιοκτησία	Ένας τρόπος να παρέχεται σε μια οντότητα το νόμιμο δικαίωμα να χρησιμοποιεί ή να μεταφέρει μια πηγή σε άλλους
Ανωνυμία	Απόκρυψη της ταυτότητας μιας οντότητας που εμπλέκεται σε μια διαδικασία
Μη-άρνηση αναγνώρισης	Παρεμπόδιση της άρνησης προηγούμενων δεσμεύσεων ή ενεργειών
Ανάκληση	Ανάκληση της πιστοποίησης ή της άδειας

Πίνακας 5.

Ένας πρωταρχικός στόχος της κρυπτογραφίας είναι να αντιμετωπίσει επαρκώς τις παραπάνω τέσσερις περιοχές τόσο στη θεωρία όσο και στην πράξη. Γενικότερα, η κρυπτογραφία σχετίζεται άμεσα με την παρεμπόδιση και τον εντοπισμό της απάτης και άλλων κακόβουλων δραστηριοτήτων. Στο Σχήμα 1 δίνεται μια σχηματική αναπαράσταση των βασικών προτεραιοτήτων της κρυπτογραφίας και πώς αυτές σχετίζονται μεταξύ τους. Οι προτεραιότητες αυτές θα πρέπει να αξιολογηθούν σε σχέση με διάφορα κριτήρια, όπως:

1. Το επίπεδο ασφάλειας. Πολλές φορές αυτό είναι δύσκολο να ποσοτικοποιηθεί. Συχνά δίνεται ως ο αριθμός των λειτουργιών που απαιτούνται για να νικηθεί το στοχευμένο αντικείμενο.
2. Η λειτουργικότητα. Τα αρχέτυπα θα χρειαστεί να συνδυαστούν, ώστε να αντιμετωπιστούν διάφορες περιπτώσεις ασφάλειας των πληροφοριών.

3. Μέθοδοι λειτουργίας. Όταν τα αρχέτυπα εφαρμόζονται με διάφορο τρόπους και με διάφορα δεδομένα εισόδου, τότε θα εμφανίσουν διαφορετικά χαρακτηριστικά. Άρα, ένα αρχέτυπο μπορεί να εμφανίσει πολύ διαφορετική συμπεριφορά και λειτουργικότητα, ανάλογα με τον τρόπο λειτουργίας του και τη χρήση του.
4. Επίδοση. Αυτό αναφέρεται στην αποτελεσματικότητα ενός αρχέτυπου σε ένα συγκεκριμένο τρόπο λειτουργίας.
5. Ευκολία υλοποίησης. Αυτό αναφέρεται στη δυσκολία να αναγνωριστεί ένα αρχέτυπο σε μια πρακτική εφαρμογή, είτε σε ένα περιβάλλον λογισμικού είτε σε ένα hardware.



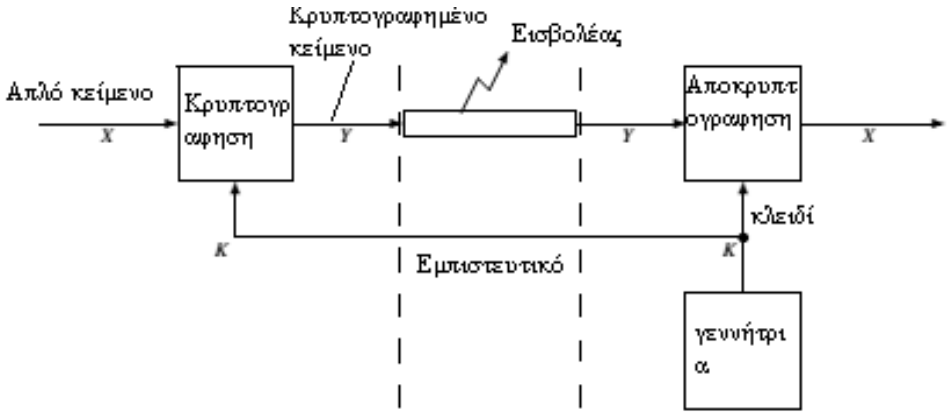
Σχήμα 1.

10.2 **Συμβατική κρυπτογραφία**

Η συμμετρική κρυπτογράφηση βασίζεται σε τρεις αλγόριθμους:

- Έναν αλγόριθμο δημιουργίας ενός κλειδιού, όπου δημιουργείται ένα μυστικό κλειδί με έναν κρυπτογραφημένο τυχαίο ή ψευδο-τυχαίο τρόπο,
- Έναν αλγόριθμο κρυπτογραφίας, ο οποίος μετατρέπει ένα απλό κείμενο σε κρυπτογραφημένο χρησιμοποιώντας ένα μυστικό κλειδί,
- Έναν αλγόριθμο αποκρυπτογράφησης, ο οποίος μετατρέπει ένα κρυπτογραφημένο κείμενο σε ένα απλό κείμενο, χρησιμοποιώντας το μυστικό κλειδί.

Η συμμετρική κρυπτογραφία επιτρέπει την εμπιστευτική επικοινωνία διαμέσου ενός ασφαλούς καναλιού, με την προϋπόθεση ότι το μυστικό κλειδί μεταφέρεται μέσω ενός ακόμα πιο ασφαλούς καναλιού. Στο σχήμα 2 αναπαρίσταται μια πιθανή χρήση αυτής της κατάστασης, όπου το μυστικό κλειδί μεταφέρεται από τον παραλήπτη στον αποστολέα με έναν εμπιστευτικό τρόπο και ο εισβολέας προσπαθεί να αντλήσει πληροφορίες μόνο από το κρυπτογραφημένο κείμενο.



Σχήμα 2.

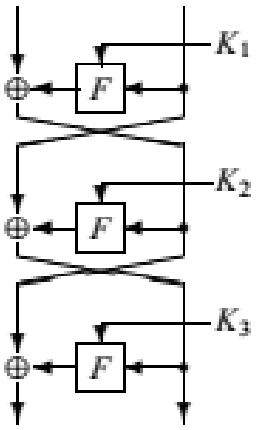
10.2.1 **To**Data Encryption Standard (DES)

ToDataEncryptionStandardπροτάθηκεαρχικά από την IBM, βασισμένο σε ένα προηγούμενο κρυπτογράφημα που αναπτύχθηκε από τον HorstFeistel και υιοθετήθηκε ως πρότυπο και εκδόθηκε το 1977. Το πρότυπο αυτό αναπτύχθηκε με βάση την ανάγκη για ασφάλεια στις ηλεκτρονικές τραπεζικές συναλλαγές. Κατά τη δεκαετία του '70 οι επιχειρήσεις που παρείχαν τεχνολογίες πληροφορίας βασίζονταν κυρίως στη βιομηχανία hardware και έτσι το πρότυπο DES είχε προοριστεί για εφαρμογές σε hardware.

Το πρότυπο DES είναι ένα μπλοκ κρυπτογράφησης. Αυτό σημαίνει ότι επιτρέπει την κρυπτογράφηση ενός μπλοκ 64-bit απλού κειμένου σε 64-bit κρυπτογραφημένου κειμένου χρησιμοποιώντας ένα μυστικό κλειδί. Πρόκειται έτσι για μια σειρά μεταθέσεων πάνω σε ένα 64-bit μπλοκ αλφαριθμητικών (string). Η κρυπτογράφηση των μηνυμάτων με τυχαίο μήκος επιτυγχάνεται μέσω ενός τρόπου λειτουργίας, ο οποίος είναι τυποποιημένος ξεχωριστά και αναλύεται παρακάτω. Το μυστικό κλειδί είναι και αυτό ένα αλφαριθμητικό 64-bit, αλλά 8 από αυτά τα bit δεν χρησιμοποιούνται καθόλου. Επομένως, συνήθως αναφέρεται ότι το DES χρησιμοποιεί κλειδιά μήκους 56bits.

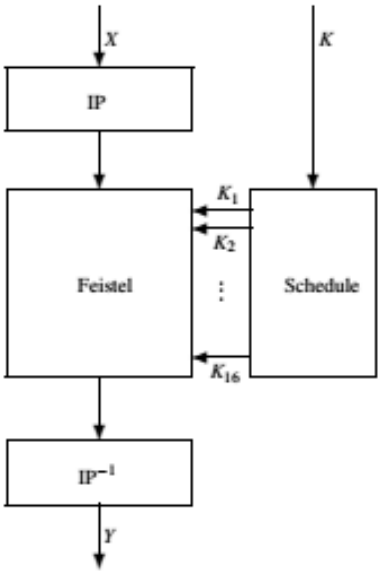
Το DES αποτελείται από μια δομή σκάλα, η οποία δημιουργεί μια μετάθεση από μια συνάρτηση. Στην πραγματικότητα, το αλφαριθμητικό εισόδου χωρίζεται σε δύο μέρη ίσου μήκους και η εικόνα του ενός τμήματος μετατρέπεται σε XOR στο άλλο τμήμα μέσω μιας κυκλικής συνάρτησης. Έτσι, υπάρχουν δύο τμήματα τα οποία μετά ανταλλάσσονται μεταξύ τους, ενώ η ενδιάμεση συνάρτηση χρησιμοποιεί υπο-κλειδιά που προέρχονται από ένα μυστικό κλειδί. Αυτή η βασική διαδικασία επαναλαμβάνεται και ο αριθμός των εφαρμογών της συνάρτησης που πραγματοποιείται ονομάζεται αριθμός κύκλων. Συνήθως αναφέρεται ως $\Psi(F_1, \ldots, F_r)$ η μετάθεση που προκύπτει από μια δομή r κύκλων, στην οποία οι κυκλικές συναρτήσεις είναι οι $F_1, \ldots, F_r$. Όλες οι συναρτήσεις F_i μπορούν να προέλθουν από

μία συνάρτηση F με την παράμετρο K_i, που ορίζεται ως υπο-κλειδί. Έτσι, ορίζεται $F_i = F^{K_i}$. Στο σχήμα 3 φαίνεται μια τέτοια δομή τριών κύκλων, όπου το πρότυπο DES αποτελείται από 16 κύκλους.



Σχήμα 3. Συνάρτηση $\Psi(F^{K_1}, F^{K_2}, F^{K_3})$

Πιο συγκεκριμένα, το DES ξεκινά με μια μετάθεση IP ενός bit, εκτελεί μια κρυπτογράφηση Feistel χρησιμοποιώντας υποκλειδιά και τέλος εκτελεί την αντίστροφη μετάθεση IP. Η διεργασία αυτή περιγράφεται σχηματικά στο σχήμα 4.

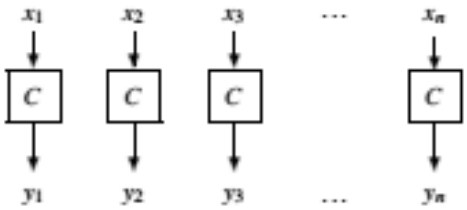


Σχήμα 4. Δομή του προτύπου DES

10.2.2 **Οι τρόποι λειτουργίας του** DES

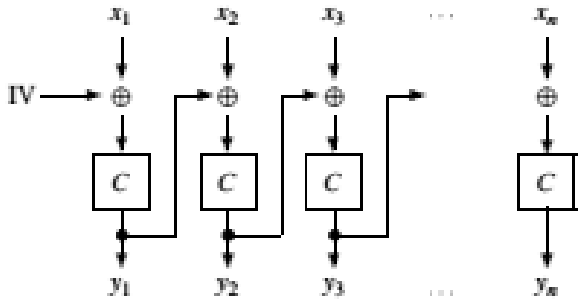
Το DES έχει την ικανότητα κρυπτογράφησης σε μπλοκ 64-bit. Προκειμένου να κρυπτογραφηθούν απλά κείμενα τυχαίου μήκους, θα πρέπει να χρησιμοποιηθεί το πρότυπο DES με έναν τρόπο λειτουργίας. Υπάρχουν διάφοροι τυποποιημένοι τρόποι, όπως αναφέρονται περιγραφικά παρακάτω:

1. ElectronicCodeBook (ECB) **à** τοαπλόκείμενοχωρίζεται σε 64-bit μπλοκ x_1, …, x_n και το κρυπτογραφημένο κείμενο y είναι η αλληλουχία των κρυπτογραφημένων μπλοκ (σχήμα 5). Εδώ υπάρχουν ορισμένα προβλήματα ασφάλειας, όπως η διαρροή πληροφοριών από την «ισότητα» των μπλοκ και προβλήματα ακεραιότητας (π.χ. να διαγραφεί ή να αντικατασταθεί ένα μπλοκ από ένα άλλο).



Σχήμα 5. ECB τρόπος λειτουργίας

2. CipherBlockChaining (CBC) **à** τοαπλόκείμενοχωρίζεται σε 64-bit μπλοκ x_1, …, x_n και το κρυπτογραφημένο κείμενο y είναι η αλληλουχία των μπλοκ που δημιουργούνται με επαναλήψεις. Υπάρχει ένα αρχικό διάνυσμα IV, που αποτελεί ένα αρχικό ψεύτικο μπλοκ, όπως φαίνεται και το σχήμα 6.



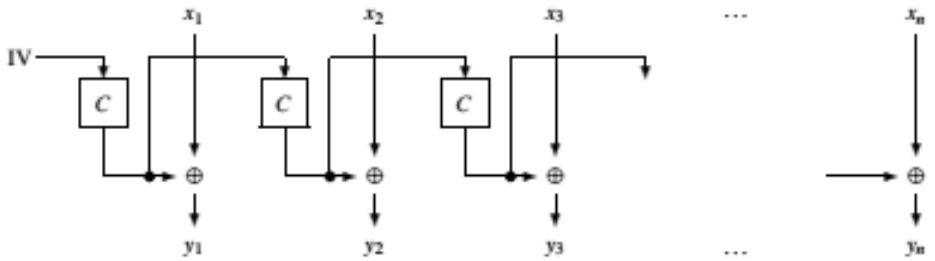
Σχήμα 6. CBC τρόπος λειτουργίας

Το αρχικό διάνυσμα δεν χρειάζεται να είναι μυστικό και υπάρχουν τέσσερις διαφορετικοί τρόποι για να χρησιμοποιηθεί το διάνυσμα αυτό:

- Η δημιουργία ενός ψευδο-τυχαίου IV το οποίο δίνεται ξεκάθαρα με το κρυπτογραφημένο κείμενο
- Η δημιουργία ενός ψευδο-τυχαίου IV το οποίο μεταφέρεται εμπιστευτικά με το κρυπτογραφημένο κείμενο

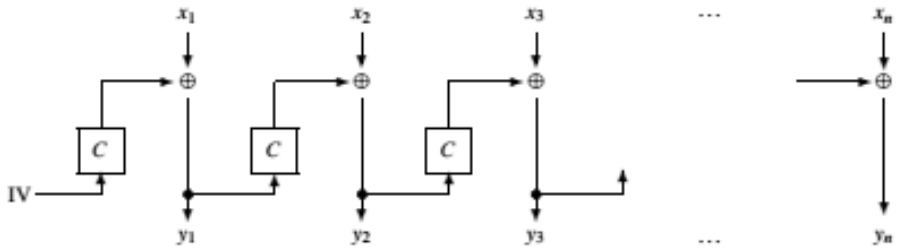
- Η χρήση ενός σταθερού IV το οποίο είναι γνωστό
- Η χρήση ενός σταθερού IV το οποίο αποτελεί τμήμα του μυστικού κλειδιού

3. OutputFeedback (OFB) **à** τοαπλόκείμενο χωρίζεται σε l -bit μπλοκ x_1, …, x_n και το κρυπτογραφημένο κείμενο y είναι η αλληλουχία των μπλοκ που δημιουργούνται με επαναλήψεις, ενώ και εδώ υπάρχει το αρχικό διάνυσμα IV, όπως φαίνεται και στο σχήμα 7.



Σχήμα 7. OFB τρόπος λειτουργίας με l ίσο με το μήκος του μπλοκ

4. CipherFeedback (CFB) **à** τοαπλόκείμενο χωρίζεται σε l -bit μπλοκ x_1, …, x_n και το κρυπτογραφημένο κείμενο y είναι η αλληλουχία των μπλοκ που δημιουργούνται με επαναλήψεις, ενώ και εδώ υπάρχει το αρχικό διάνυσμα IV, όπως φαίνεται και στο σχήμα 8.

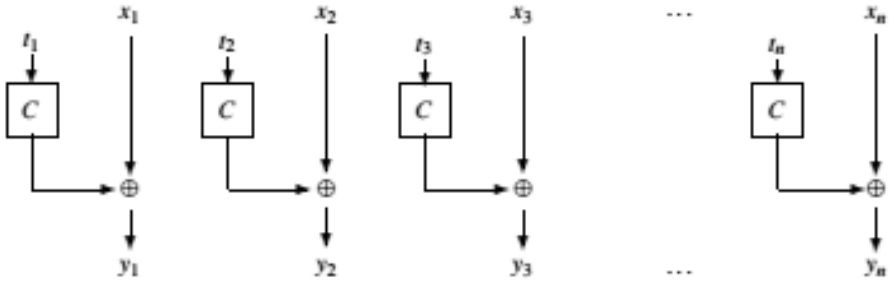


Σχήμα 7. CFB τρόπος λειτουργίας με l ίσο με το μήκος του μπλοκ

5. CounterMode (CTR) **à** τοαπλόκείμενο χωρίζεται σε l -bit μπλοκ x_1, …, x_n και το κρυπτογραφημένο κείμενο y είναι η αλληλουχία των μπλοκ που δημιουργούνται με επαναλήψεις. Εδώ χρησιμοποιείται μια σειρά από μετρητές t_1, …, t_nκαι η κρυπτογράφηση πραγματοποιείται ως:

$$y_i = x_i \oplus truncL_l(C(t_i))$$

Στο σχήμα 8 δίνεται ο τρόπος λειτουργίας του CFB όπου το l είναι ίσο με το μήκος του μπλοκ.



Σχήμα 8. CTR τρόπος λειτουργίας με l ίσο με το μήκος του μπλοκ

10.2.3 StreamCiphers

Όλα τα συμβατικά συστήματα κρυπτογράφησης που περιγράφηκαν παραπάνω εκτελούν κρυπτογράφηση κατά μπλοκ, που σημαίνει ότι κρυπτογραφούν μια ομάδα (block) απλών κειμένων. Αντίθετα, η κρυπτογράφηση κατά ροή (streamcipher) συνήθως γίνεται σε μια ροή bit απλού κειμένου μικρότερου μεγέθους.

Ένα streamcipher παράγει μια ακολουθία κλειδιών που λέγονται key-stream και χρησιμοποιείται σαν ένα one-timepad, δηλαδή χρησιμοποιείται ένα ψευδο-τυχαίο κλειδί που παράγεται ως ένα key-stream. Επίσης, ένα blockcipher μπορεί να μετατραπεί σε streamcipher χρησιμοποιώντας τους τρόπους λειτουργίας CFBή CTR με μια μικρή παράμετρο l[9].

Ο αλγόριθμος κρυπτογράφησης RC4 εμφανίστηκε το 1994 και χρησιμοποιείται ευρέως στο SSL/TLS και συγκεκριμένα μερικά προγράμματα περιήγησης διαδικτύου και κάποιοιservers μπορεί να χρησιμοποιούν το RC4 ως τον προεπιλεγμένο αλγόριθμο κρυπτογράφησης για να προστατεύονται οι συναλλαγές. Ο αλγόριθμος αυτός λειτουργεί διαβάζοντας ένα απλό κείμενο (plaintext) σαν ένα bytestream και παράγει ένα κρυπτογραφημένο κείμενο σαν ένα bytestream. Η καρδιά του αλγόριθμου είναι μια γεννήτρια key-stream που χρησιμοποιείται για τον αλγόριθμο one-timepad.

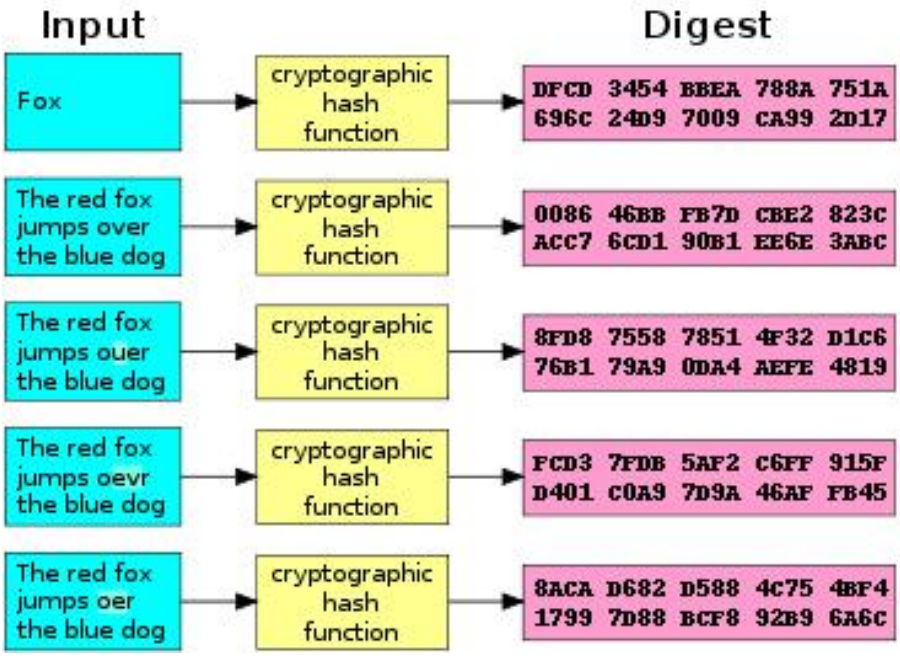
Ο αλγόριθμος A5/1 αποτελεί ένα άλλο streamcipher που χρησιμοποιείται στα GSM δίκτυα κινητής τηλεφωνίας. Χρησιμοποιείται για να προσφέρει ασφάλεια στις τηλεφωνικές κλήσεις κατά τη σύνδεση του κινητού τηλεφώνου με το βασικό σταθμό.

Ο αλγόριθμος E0 είναι ένα streamcipher που χρησιμοποιείται στο πρότυπο Bluetooth και, όπως και ο A5/1, παράγει key-streams που, μέσω της πράξης XOR, δημιουργείται το απλό κείμενο.

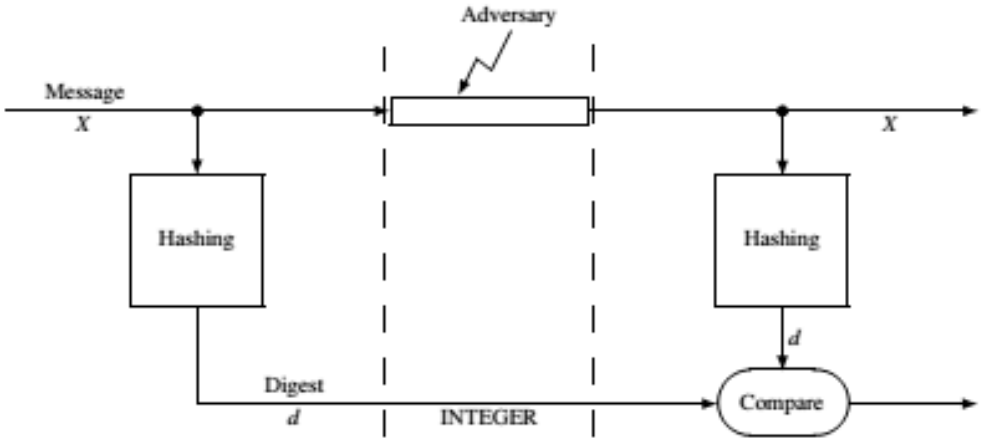
10.2.4 CryptographicHashing

Στην επιστήμη των υπολογιστών, οι hashfunctionsχρησιμοποιούνται για να ρυθμίσουν μια βάση δεδομένων, έτσι ώστε να υπάρχει αποτελεσματική πρόσβαση στα στοιχεία του. Μια είσοδος είναι συνήθως ένα ζεύγος (x, y),όπου το x είναι το σήμα εισόδου και το y είναι τα δεδομένα. αποθηκεύεται στη θέση h(x) στη βάση δεδομένων. Αργότερα, αν χρειαστεί να υπάρχει πρόσβαση στα δεδομένα που σχετίζονται με την ετικέτα x, τότε απλά ελέγχεται η τοποθεσία h (x). Τα διάφορα προβλήματα προκύπτουν όταν υπάρχουν δύο διαφορετικές ετικέτεςx και x', όπου h(x) = h (x'), πράγμα που ονομάζεται σύγκρουση (collision). Μια hash function είναι αποτελεσματική όταν το domainspace τους είναι μικρό και ο αναμενόμενος αριθμός συγκρούσεων είναι μικρός σε πρακτικές εφαρμογές.

Στην κρυπτογραφία, οι hashfunctions χρησιμοποιούνται για να προστατεύσουν την ακεραιότητα των δεδομένων, δηλαδή αντί να προστατεύεται η ακεραιότητα δεδομένων τυχαίου μεγέθους, είναι επιθυμητό να συγκεντρώνεται η προστασία σε μικρές ακολουθίες bit. Έτσι, τα δεδομένα πρέπει να μετατραπούν σε ένα αλφαριθμητικό καθορισμένου μεγέθους που λέγεται hashvalue (Σχήμα 9). Αν υποτεθεί ότι η προστασία του hashvalue έχει επιτευχθεί, τότε μπορεί να γίνει ανίχνευση για πιθανή αλλοίωση των δεδομένων χρησιμοποιώντας ξανά την hashfunction και συγκρίνοντας τις δύο hashvalues. Τότε, μπορεί να χρησιμοποιηθεί ένα κανάλι για να παρέχεται ακεραιότητα στα δεδομένα που μεταφέρονται μέσω ενός μη ασφαλούς καναλιού (Σχήμα 10). Έτσι, για λόγους ασφαλείας θα πρέπει να εξασφαλιστεί ότι είναι αδύνατον να υπάρξει μεταβολή ή αλλοίωση του περιεχομένου των δεδομένων στο αποτέλεσμα της hashfunction.



Σχήμα 9. Μια hash function κρυπτογραφίας



Σχήμα 10. Κανάλι ακεραιότητας των δεδομένων

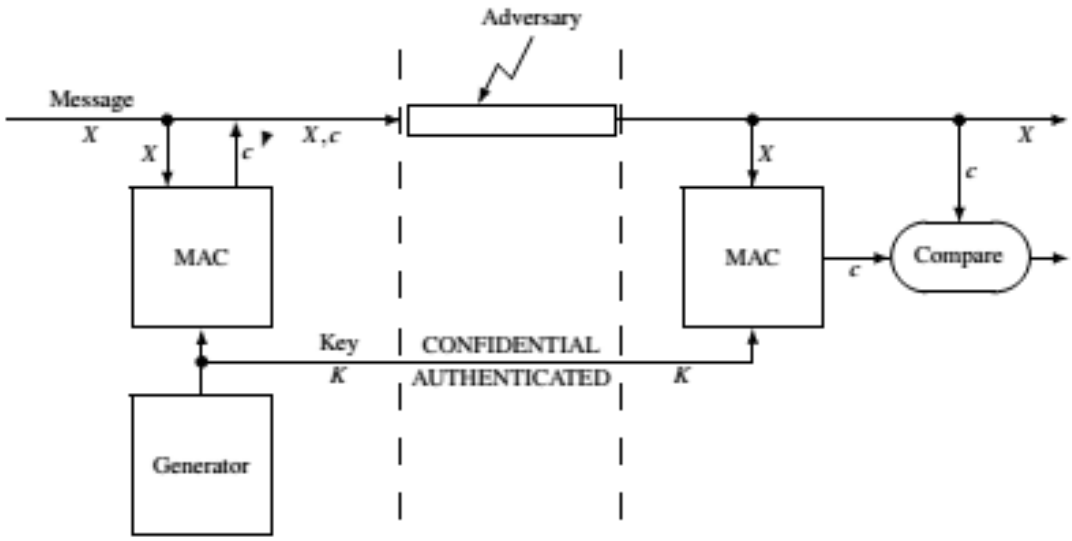
Ένα παράδειγμα μιας κρυπτογραφικής hashfunction είναι το MD5 (MessageDigest) που δημοσιεύτηκε το 1992 και χρησιμοποιείται ευρέως σε εφαρμογές Internet. Η συνάρτηση αυτή κρυπτογραφεί αλφαριθμητικά τυχαίου μήκος σε 128 bits. Η συνάρτηση συμπίεσης είναι μια συνάρτηση κρυπτογράφησης C_0 η οποία

απεικονίζει μια τιμή H=(A, B, C, D) 128-bit και ένα keyblock 512-bit σε μια 128-bittιμή.

Ένα άλλο πολύ γνωστό παράδειγμα μιας κρυπτογραφικής συνάρτησης είναι η SHA (SecureHashAlgorithm), που δημοσιεύτηκε από την Αμερικανική κυβέρνηση το 1993. Βασίζεται στο MD5 και χρησιμοποιείται κυρίως σε εφαρμογές ψηφιακής υπογραφής. Μετατρέπει τα δεδομένα σε 160 bits και χρησιμοποιεί τη συνάρτηση συμπίεσης 160×512 **à** 160. Η αρχική έκδοση αντικαταστάθηκε το 1995 από μια άλλη, ελαφρώς διαφορετική, την SHA-1, μάλλον για λόγους ασφαλείας. Η συνάρτηση συμπίεσης είναι μια συνάρτηση κρυπτογράφησης C_0 η οποία απεικονίζει μια τιμή H=(A, B, C, D, E) 160-bit και ένα keyblock 512-bitB=(x_0,…,x_{15}) σε μια 160-bittιμή.

10.2.5 MessageAuthenticationCode

OMessageAuthenticationCode (MACs) είναιένασκώδικαςπουεγγυάται την αυθεντικότητα και ακεραιότητα ενός μηνύματος που μεταφέρεται διάμεσο ενός μη ασφαλούς καναλιού. Αν αυτό γίνει με χρήση ενός κρυπτογραφικού hashfunction, τότε το hashvalue θα πρέπει να μεταδοθεί μέσω ενός ασφαλούς καναλιού που εξασφαλίζει την αυθεντικότητα. Όπως γίνεται και με την κρυπτογράφηση, η χρήση αυτού του καναλιού μπορεί να διασπαστεί και να χρησιμοποιηθεί για να μεταφέρει ένα μυστικό κλειδί και καμία τιμή εξαρτώμενη από το μήνυμα. Όταν εγκατασταθεί το κλειδί, τότε η μετάδοση του hashvalueαντικαθίσταται από την μετάδοση του MAC μέσω του μη ασφαλούς καναλιού. Τότε, μπορεί να χρησιμοποιηθεί ένα κανάλι αυθεντικότητας για να πιστοποιεί το μήνυμα, όπως φαίνεται στο Σχήμα 11.



Σχήμα 11. Κανάλι αυθεντικότητας

Υπάρχουν τρεις διαφορετικοί τύποι MAC, που αναφέρονται παρακάτω:

(1) Τα MACβασιζόμενα σε blockciphers (CBC-MAC)

Αποτελούν μια αρκετά γνωστή δομή, τη δομή CBC-MAC, όπου η ιδέα είναι να λαμβάνεται το τελευταίο κρυπτογραφημένο block από την CBC κρυπτογράφηση του μηνύματος ως MAC. Παρόλα αυτά, η ιδέα αυτή δεν είναι απόλυτα ασφαλής.

(2) Τα MAC βασιζόμενα σε streamciphers

Ένας MAC αλγόριθμος στην ουσία είναι μια τυχαία hashfunction η διανομή της οποίας καθορίζεται από την επιλογή ενός μυστικού κλειδιού. Μπορεί να δημιουργηθεί ένα ασφαλές MAC από μια γενική hashfunction, κρυπτογραφώντας απλά την έξοδο με ένα Vernamcipher.

(3) Τα MAC βασιζόμενα σε hash functions (HMAC)

Το να δημιουργηθεί μια hashfunction από έναν αλγόριθμο MAC είναι σχετικά απλό, χρειάζεται ένα σταθερό κλειδί. Εντούτοις, θα πρέπει να λαμβάνεται υπόψη ότι το MAC δεν μπορεί να προσφέρει προστασία ενάντια σε επιθέσεις

σύγκρουσης. Μπορεί όμως να δημιουργηθεί MAC από κρυπτογραφημένες hashfunctions. Η δομή αυτή, που λέγεται HMAC, δημιουργήθηκε χάρη στους MihirBellare, RanCanettiκαι HugoKrawczyk. Το κλειδί χρησιμοποιείται για να κρυπτογραφήσει το messagedigest του μηνύματος. Ο παραλήπτης, που μοιράζεται με τον αποστολέα το ίδιο κλειδί, αποκρυπτογραφεί το messagedigest και μετά το συγκρίνει με ένα άλλο messagedigest που παράγει ο ίδιος από το μήνυμα. Εάν η σύγκριση είναι επιτυχής, τότε ο παραλήπτης είναι σίγουρος ότι δεν έχουν αλλοιωθεί τα δεδομένα.

10.3 **ΑσύμμετρηΚρυπτογραφία** (Public-key Cryptography)

Η επινόηση της ασύμμετρης κρυπτογραφίας αποδίδεται συχνά στους WhitfiledDiffie και MartinHellman, που δημοσιεύτηκε σε μια εργασία τους το 1976, δίνοντας νέα διάσταση στην κρυπτογραφία.

Ένα σύστημα ασύμμετρης κρυπτογραφίας ορίζεται ως:

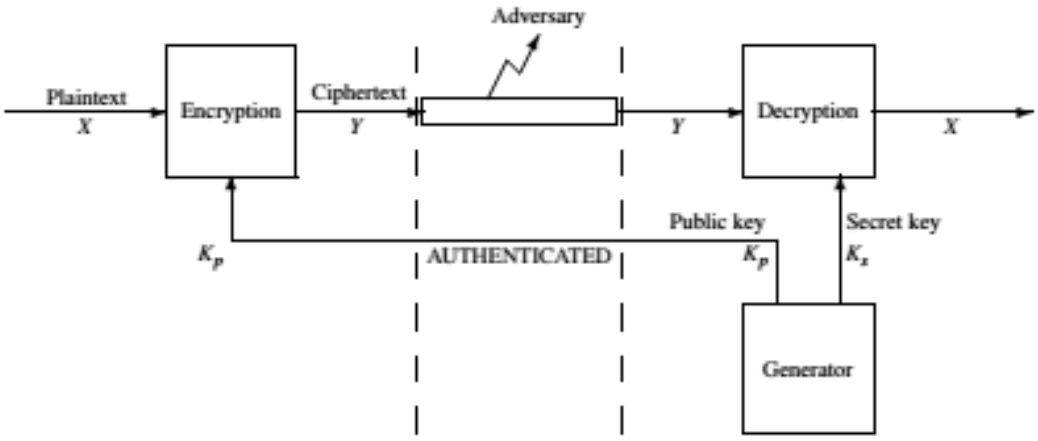
1. Ένα μέσο παραγωγής ψευδο-τυχαίων κλειδιών Gen: πρόκειται για ένα στοχαστικό αλγόριθμο που παράγει ένα ζεύγος κλειδιών (K_p, K_s), όπου το K_p είναι το publickey και το K_s είναι το secretkey.
2. Ένας αλγόριθμος κρυπτογράφησης Enc: είναι ένας αλγόριθμος (που μπορεί να είναι και στοχαστικός) που παράγει ένα κρυπτογραφημένο κείμενο Y από μια είσοδο απλού κειμένου (plaintext) X και ένα publickeyK_p.
3. Ένας αλγόριθμος απο-κρυπτογράφησης Dec: είναι ένας αλγόριθμος (που υποχρεωτικά υλοποιεί μια προσδιορισμένη συνάρτηση) που παράγει ένα απλό κείμενο X από ένα κρυπτογραφημένο κείμενο Y και ένα secretkeyK_s.

Με αυτό τον τρόπο, η κρυπτογράφηση δεν είναι αναγκαίο να είναι ένα προς ένα, καθώς μπορεί να υπάρχουν πολλά κρυπτογραφημένα κείμενα (ciphertexts) που να

αντιστοιχούν στο ίδιο απλό κείμενο (plaintext). Παρόλα αυτά, ένα σύστημα κρυπτογράφησης θα πρέπει να πλήρη τις παρακάτω απαιτήσεις:

- Για κάθε ζεύγος κλειδιών που παράγεται (K_p, K_s) οποιοδήποτε απλό κείμενο x και οποιαδήποτε πιθανή έξοδος y από το $Enc_{Kp}(x)$, θα πρέπει να έχει $Dec_{Ks}(y)=x$.
- Έχοντας πρόσβαση στις προδιαγραφές K_p και ένα Dec_{Ks}, τότε είναι δύσκολο να αποκρυπτογραφηθεί ένα κρυπτογραφημένο κείμενο y που έχει παραχθεί, χωρίς να σταλεί η απορία y στην $Dec_{Ks.}$

Στο σχήμα 12 παρακάτω φαίνεται το μοντέλο κρυπτογράφησης Shannon που έχει διαμορφωθεί για συστήματα κρυπτογράφησης public-key. Έτσι, μπορεί να μετατραπεί ένα μη ασφαλές κανάλι σε έμπιστο με τη χρήση της publickey κρυπτογραφίας, ενώ μπορεί να υπάρχει και ένα επιπλέον κανάλι για να μεταδίδεται το publickey (συνήθως η παραγωγή των κλειδιών γίνεται από τον παραλήπτη). Το κανάλι αυτό όμως δεν είναι έμπιστο και απαιτείται πιστοποίηση, που σημαίνει ότι ο αποστολέας του κρυπτογραφημένου μηνύματος θα πρέπει να είναι σίγουρος ότι το publickey που χρησιμοποιεί είναι το κατάλληλο κλειδί.



Σχήμα 12. Ασύμμετρη κρυπτογραφία

Όπως φαίνεται, η κρυπτογράφηση και η απο-κρυπτογράφηση είναι στην ουσία ασύμμετρα. Αυτό σημαίνει ότι μόνο ο παραλήπτης του κρυπτογραφημένου μηνύματος χρειάζεται να έχει πρόσβαση στο μυστικό κλειδί για να μπορέσει να αποκρυπτογραφήσει το κείμενο. Στην συμβατική κρυπτογραφία, το μυστικό κλειδί έπρεπε να χρησιμοποιηθεί τόσο για την κρυπτογράφηση όσο και για την απο-κρυπτογράφηση, ενώ η απο-κρυπτογράφηση ήταν ουσιαστικά η ίδια διαδικασία με την κρυπτογράφηση, αλλά ανάποδα. Αντίθετα, στην ασυμμετρία δεν απαιτείται να υπάρχει πρόσβαση σε κάποιο μυστικό κλειδί για να κρυπτογραφηθεί ένα μήνυμα. Επιπλέον, το μυστικό κλειδί αποτελεί μυστικό μόνο για ένα χρήστη και όχι μυστικό για δύο χρήστες, όπως συμβαίνει στη συμβατική κρυπτογραφία.

Όπως είναι φυσικό, το κέρδος αυτό της ασύμμετρης κρυπτογραφίας έχει ένα κόστος: τα συστήματα κρυπτογράφησης publickey απασχολούνται περισσότερο, τόσο με την έννοια της κατανόησης από τους χρήστες αλλά και οι ίδιοι οι υπολογιστές απασχολούνται περισσότερο.

10.3.1 **Πρότυπα** RSA

Τα πρότυπα της ασύμμετρης κρυπτογραφίας (Public-KeyCryptographyStandards – PKCS) αποτελούν ένα σετ αλγορίθμων που βασίζονται στον αλγόριθμο RSA.

Έχοντας ένα modulusNμεγέθους kbytes, προκειμένου να κρυπτογραφηθεί ένα μήνυμα M μήκους το πολύ k-11 bytes, ακολουθείται η παρακάτω διαδικασία:

1. Παράγεται ένα αλφαριθμητικό PS από ψευδο-τυχαία μη μηδενικά bytes, έτσι ώστε το μήνυμα συνεχόμενα με το PS να έχει συνολικό μήκος k-3 bytes.
2. Κατασκευάζεται το byte αλφαριθμητικό προσθέτοντας στη σειρά ένα μηδενικό byte, ένα byte ίσο με 2, το PS, ένα ακόμα μηδενικό byte και μετά το μήνυμα. Αυτό γράφεται 00 | | 02 | | PS | | 00 | | M.
3. Αυτό το αλφαριθμητικό των bytes μετατρέπεται σε ακέραιο αριθμό.

4. Υπολογίζεται η απλή RSA κρυπτογράφηση.
5. Γίνεται μετατροπή του αποτελέσματος σε ένα αλφαριθμητικό kbytes

Στη συνέχεια, η διαδικασία απο-κρυπτογράφησης είναι απλή:

1. Μετατρέπεται το κρυπτογραφημένο κείμενο σε ακέραιο αριθμό. Το αποτέλεσμα απορρίπτεται αν είναι μεγαλύτερο από το αρχικό modulusN.
2. Εκτελείται ο απλός αλγόριθμος απο-κρυπτογράφησης RSA και ανακτάται ένας ακόμα ακέραιος.
3. Μετατρέπεται ο ακέραιος πίσω σε αλφαριθμητικό byte.
4. Ελέγχεται αν το αλφαριθμητικό έχει τη μορφή 00||02||PS||00||M για μερικά bytestringsPSκαι M, όπου το PS δεν έχει μηδενικά bytes.
5. Παράγεται το αποτέλεσμα M.

Παρόλο που ένα σύστημα κρυπτογράφησης RSA θεωρείται σχετικά ισχυρό, εντούτοις υπάρχουν διάφοροι τρόποι για να το καταστήσουν μη ασφαλές. Μερικοί από αυτούς δίνονται επιγραμματικά παρακάτω:

- Επίθεση στην αναμετάδοση μιας κρυπτογράφησης με χαμηλό εκθετικό κρυπτογράφησης. Ας υποτεθεί ότι ο αποστολέας θέλει να αναμεταδώσει το ίδιο μήνυμα x σε n διαφορετικούς παραλήπτες που έχουν publickeys (e, N_1), …, (e, N_n) με το ίδιο χαμηλό εκθετικό e. Ο αποστολέας πρέπει να στείλει $y_i = x^e \bmod N$στον i-οστό παραλήπτη, για i = 1,…, n. Αν n>e, τότε είναι σχετικά εύκολο να αποκρυπτογραφηθούν όλα τα αντίστοιχα ciphertexts$y_1,\ldots,y_n$.
- Επιθέσεις στο χαμηλό εκθέτη. Οι χαμηλοί εκθέτες έχουν πολλά μειονεκτήματα, όπου ξεχωρίζουν τα χαμηλά e και τα χαμηλά d. Όταν το e είναι χαμηλό, τότε υπάρχουν επιθέσεις χάρη στον DonCoppersmith ενάντια

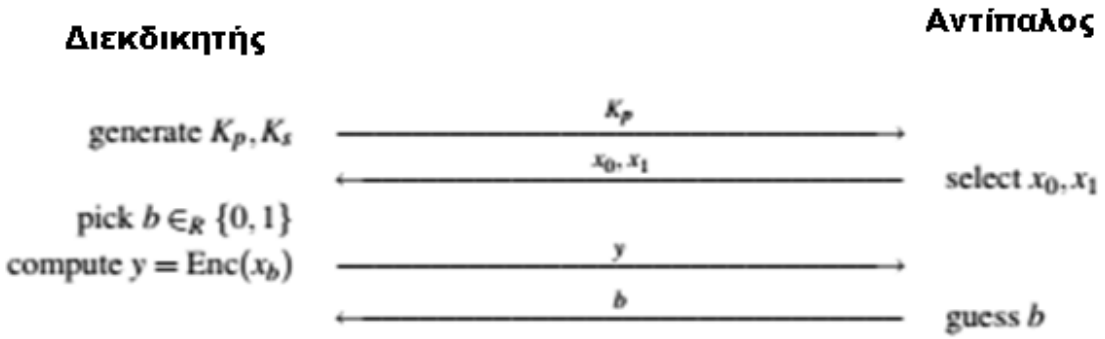
σε διάφορες χρήσεις του RSA. Όταν το d είναι χαμηλό, τότε υπάρχει ένας αλγόριθμος που οφείλεται στον MichaelWiener, ο οποίος καθιστά ικανή την ανάκτηση του μυστικού κλειδιού.

- Πλευρικές επιθέσεις. Υπάρχουν πολλοί τρόποι για να πάρει κάποιος πλευρικές πληροφορίες με σκοπό να μπορέσει να σπάσει το RSA. Ένας από αυτούς είναι το differentialfaultanalysis, όπου η επίθεση γίνεται με πιο δραστήριους τρόπους για να ληφθούν πληροφορίες, όπως η φυσική πίεση της μηχανής (με θερμότητα, ακτίνες, αλλοιωμένο ρεύμα εισόδου κτλ). Ένας πιο αποτελεσματικός τρόπος για να ληφθούν πλευρικές πληροφορίες είναι να μετρηθεί ο χρόνος υπολογισμού. Μερικοί μικρο-επεξεργαστές έχουν μια οδηγία πολλαπλασιασμού όπου ο χρόνος υπολογισμού του εξαρτάται από τους τελεστές εισόδου. Έχει αποδειχτεί από τον PaulKocher ότι αυτή η πληροφορία μπορεί να χρησιμοποιηθεί με σκοπό να ανακτηθούν κάποιες πληροφορίες σχετικά με τους εσωτερικούς υπολογισμούς και μετά να ανακτηθούν και τα μυστικά κλειδιά.

Έχοντας αναφέρει τους παραπάνω τρόπους επίθεσης σε ένα σύστημα με ασύμμετρη κρυπτογράφηση, παραμένει η ερώτηση σχετικά με το ποιες θα πρέπει να είναι οι ελάχιστες προϋποθέσεις που θα τηρούνται από το σύστημα, ώστε αυτό να είναι ασφαλές. Υπάρχουν τόσα πολλά σενάρια επιθέσεων, που η αρχική έννοια της ασφάλειας με την κρυπτογράφηση, δηλαδή η υπολογιστική δυσκολία της απο-κρυπτογράφησης, να μην είναι πλέον επαρκής. Σήμερα, υπάρχουν δύο γνωστές έννοιες ασφάλειας και τρεις έννοιες αντιπάλων, έτσι δίνονται έξι πιθανοί ορισμοί.

Αρχικά, οιShafiGoldwasserκαιSilvioMicali πρότειναν την έννοια semanticsecurity. Η έννοια αυτή σημαίνει ότι το κρυπτογραφημένο κείμενο δεν περιέχει κανένα ενδιαφέρον bit πληροφορίας που να σχετίζεται με το plaintext. Η έννοια αυτή περιγράφεται σαν παιχνίδι ανάμεσα στον διεκδικητή και τον αντίπαλο και η ροή του είναι ως εξής (Σχήμα 13):

1. Αρχικά δίνεται το σύστημα κρυπτογράφησης στον διεκδικητή και στον αντίπαλο
2. Ο διεκδικητής παράγει ένα ζεύγος public και secretkeys και αποκαλύπτει το publickey
3. Ο αντίπαλος επιλέγει δύο plaintextsx$_0$και x$_1$ και τα στέλνει στον διεκδικητή
4. Ο διεκδικητής επιλέγει τυχαία ένα bitb. Το κρυπτογραφεί x$_b$ και στέλνει το ciphertextyστον αντίπαλο
5. Ο αντίπαλος προσπαθεί να μαντέψει το b



Σχήμα 13.

Όταν το σύστημα κρυπτογράφησης είναι ασφαλές, τότε ο αντίπαλος δεν μπορεί να μαντέψει το b και έτσι δεν μπορεί να γίνει διάκριση ανάμεσα στα δύο μηνύματα.

Μια άλλη έννοια ασφάλειας είναι η nonmalleability (NM), η οποία περιγράφεται πάλι σαν παιχνίδι, αλλά λίγο πιο πολύπλοκο από το semanticsecurity.

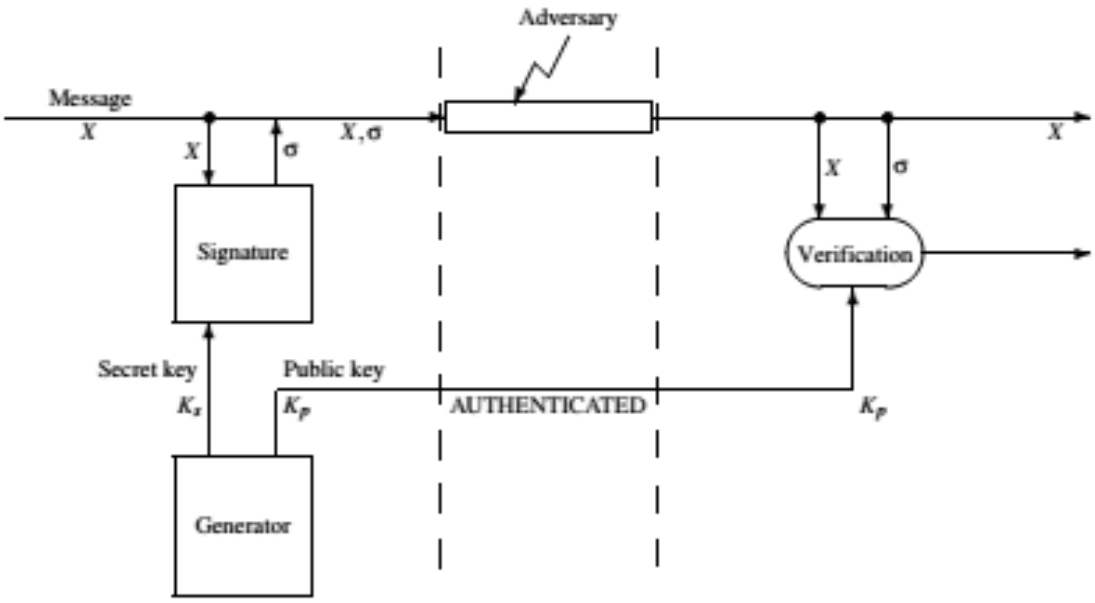
10.4 **Ψηφιακή Υπογραφή**

Τα ασύμμετρα συστήματα κρυπτογράφησης αποτελούν μια εναλλακτική στη συμβατική κρυπτογραφία. Με την ίδια λογική, υπάρχει μια εναλλακτική στους MAC αλγόριθμους, που είναι η έννοια της ψηφιακής υπογραφής. Με την ψηφιακή υπογραφή δίνεται ένα μυστικό κλειδί σε κάθε χρήστη και ένα αντίστοιχο publickey ελευθερώνεται. Ο χρήστης μπορεί να υπογράψει οποιοδήποτε μήνυμα και οποιοσδήποτε άλλος μπορεί να πιστοποιήσει την ορθότητα αυτής της υπογραφής.

10.4.1 **Συστήματα Ψηφιακής Υπογραφής**

Ένα σύστημα ψηφιακής υπογραφής αποτελείται από (Σχήμα 14):

1. Ένα μέσο παραγωγής ψευδο-τυχαίων κλειδιών όπου παράγεται ένα publickeyK_pκαι έναsecretkeyK_s.
2. Ένας αλγόριθμος υπογραφής, ο οποίος από κάθε μήνυμα Χ και από το μυστικό κλειδίK_s υπολογίζει (με ντετερμινιστικό ή με στοχαστικό τρόπο) μια υπογραφή σ.
3. Ένας αλγόριθμος πιστοποίησης, ο οποίος από κάθε μήνυμα Χ, την υπογραφή σ και το publickeyK_p πιστοποιεί (με ντετερμινιστικό τρόπο) την ορθότητα της υπογραφής.



Σχήμα 14. Ψηφιακές υπογραφές

Οι ψηφιακές υπογραφές παρόλα αυτά, αντιμετωπίζουν διάφορα θέματα ασφάλειας:

1. Πρέπει να παρέχουν έλεγχο της αυθεντικότητας και ακεραιότητα. Για το λόγο αυτό, θα πρέπει να είναι αδύνατον για τον οποιονδήποτε που δεν έχει πρόσβαση στο μυστικό κλειδί να πλαστογραφήσει ένα ζεύγος (X, σ), που να είναι έγκυρο και να αντιστοιχεί στο publickey. Αυτό ονομάζεται πλαστογράφηση υπογραφής (signatureforgery). Φυσικά, αυτή η υπόθεση θα πρέπει να παραμένει έγκυρη ακόμα και αν ο αντίπαλος έχει περισσότερα έγκυρα ζεύγη (X, σ). Εδώ διακρίνονται διάφορες κλάσεις επιθέσεων που συνοψίζονται παρακάτω από την πιο ισχυρή στην πιο αδύναμη.
    a. *Totalbreak*: ο αντίπαλος καταφέρνει να ανακτήσει το μυστικό κλειδί απόέναpublickey, το οποίο μπορεί να χρησιμοποιηθεί για να πλαστογραφήσει υπογραφές.

b. *Universalforgery*: ο αντίπαλος καταφέρνει να αντλήσει έναν αλγόριθμο χρησιμοποιώντας ένα publickey, ο οποίος καθιστά ικανή την πλαστογράφηση της υπογραφής για οποιοδήποτε μήνυμα (ή για ένα τυχαίο μήνυμα).
c. *Selectiveforgery*: ο αντίπαλος μπορεί να παράγει μηνύματα Χ, με τον ίδιο τρόπο όπως με το publickey, να πλαστογραφήσει μια υπογραφή απο ένα επιλεγμένο μήνυμα. (Σημείωση: η επιλογή του μηνύματος-στόχου γίνεται πριν μάθει ποιο είναι το publickey).
d. *Existentialforgery*: χρησιμοποιώνταςέναpublickey ο αντίπαλος μπορεί να δημιουργήσει ένα ζεύγος από ένα μήνυμα Χ και μια πλαστογραφημένη υπογραφή, αλλά δεν έχει έλεγχο στο ποιο Χ θα έχει σαν έξοδο η επίθεση.

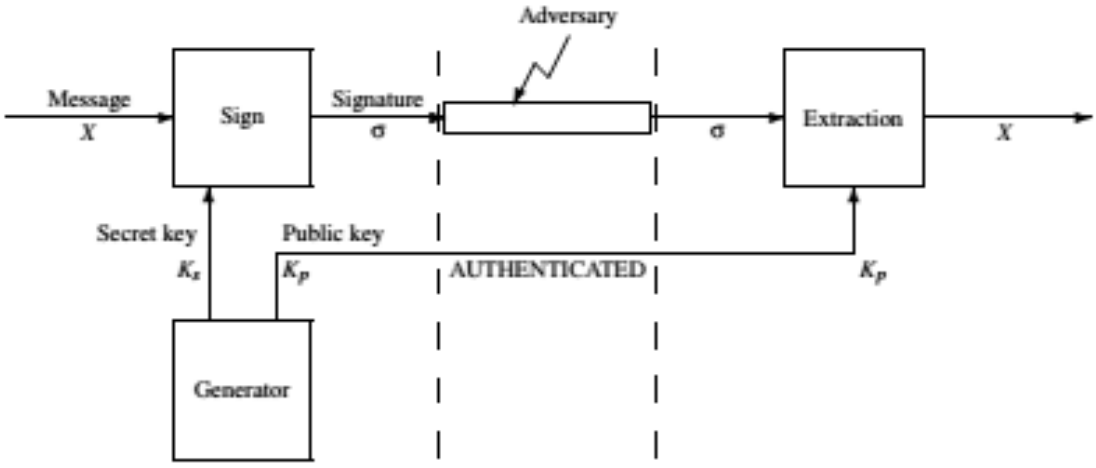
2. Πρέπει να παρέχουν μη-αποποίηση. Θα πρέπει να είναι αδύνατο για το νόμιμο χρήστη της υπογραφής να μπορεί να αποποιηθεί την υπογραφή του. Όταν ένα υπογεγραμμένο μήνυμα (Χ, σ) είναι έγκυρο, τότε ο φέρων την υπογραφή δεν μπορεί να ισχυριστεί ότι η υπογραφή έχει πλαστογραφηθεί. Στην πραγματικότητα, αν η υπογραφή είναι ασφαλής ως προς τις επιθέσεις που αναφέρθηκαν παραπάνω, τότε είναι αδύνατον για τον αντίπαλο να πλαστογραφήσει το μήνυμα, και έτσι η υπογραφή δεν μπορεί να έχει δημιουργηθεί από άλλον πέραν από αυτόν που έχει το μυστικό κλειδί. Εδώ πρέπει να σημειωθεί ότι αυτός που έχει το κλειδί είναι ένα και μόνο άτομο, πράγμα που αποτελεί κρίσιμο θέμα για τις υπογραφές και δεν υφίσταται στην κρυπτογράφηση. Τέλος, η μη-αποποίηση βασίζεται στην υπόθεση ότι καμία επίθεση δεν είναι εφικτή.

10.4.2 **Υπογραφή** RSA

Υπάρχει τρόπος ώστε ο αλγόριθμος RSA μπορεί να χρησιμοποιηθεί σαν σύστημα ψηφιακής υπογραφής. Η σχέση ανάμεσα στα ασύμμετρα συστήματα κρυπτογράφησης και τις ψηφιακές υπογραφές είναι γενικότερη και δεν εξειδικεύεται στο RSA.

- **Από τα ασύμμετρα συστήματα κρυπτογράφησης στις Ψηφιακές υπογραφές**.

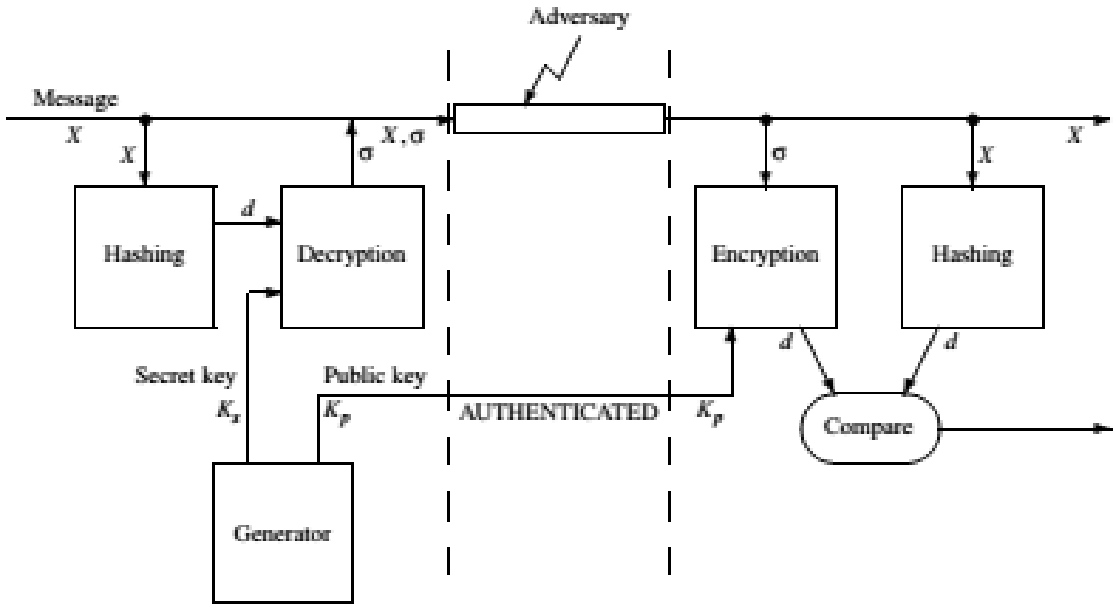
  Αν υποτεθεί ότι υπάρχει ένα ασύμμετρο σύστημα κρυπτογράφησης με ένα μέσο παραγωγής κλειδιών, έναν αλγόριθμο κρυπτογράφησης, ο οποίος είναι ντετερμινιστικός, και έναν αλγόριθμο απο-κρυπτογράφησης, τότε μπορεί να υπογραφεί ένα μήνυμα απο-κρυπτογραφώντας το. Εδώ υπάρχει υπογραφή με ανάκτηση μηνύματος (messagerecovery), που σημαίνει ότι δεν χρειάζεται να σταλεί το X μαζί με το σ, αφού το X μπορεί να προκύψει από το σ. Έτσι, ο αλγόριθμος πιστοποίησης μπορεί να αντικατασταθεί από έναν αλγόριθμο εξαγωγής. Η περίπτωση αυτή απεικονίζεται στο σχήμα 15.



Σχήμα 15. Ψηφιακή υπογραφή με ανάκτηση μηνύματος

Προκειμένου να μειωθεί το μέγεθος της υπογραφής, μπορεί να χρησιμοποιηθεί μια hashfunction πριν την υπογραφή. Αυτή τη hashfunction θα πρέπει να είναι collision-resistant, ειδάλλως μπορεί να υπάρχει η ίδια υπογραφή σε δύο διαφορετικά μηνύματα, με αποτέλεσμα μια επίθεση στο πρώτο μήνυμα να δημιουργεί πλαστογράφηση της υπογραφής στο δεύτερο μήνυμα.

Στο σχήμα 16 παρουσιάζεται ο γενικός μετασχηματισμός μιας ασύμμετρης κρυπτογράφησης σε ένα σύστημα υπογραφής. Εδώ δεν παρέχεται ανάκτηση μηνύματος.



Σχήμα 16. Μετατροπή από κρυπτογράφηση σε υπογραφή

- **Η απλή** RSA **υπογραφή**

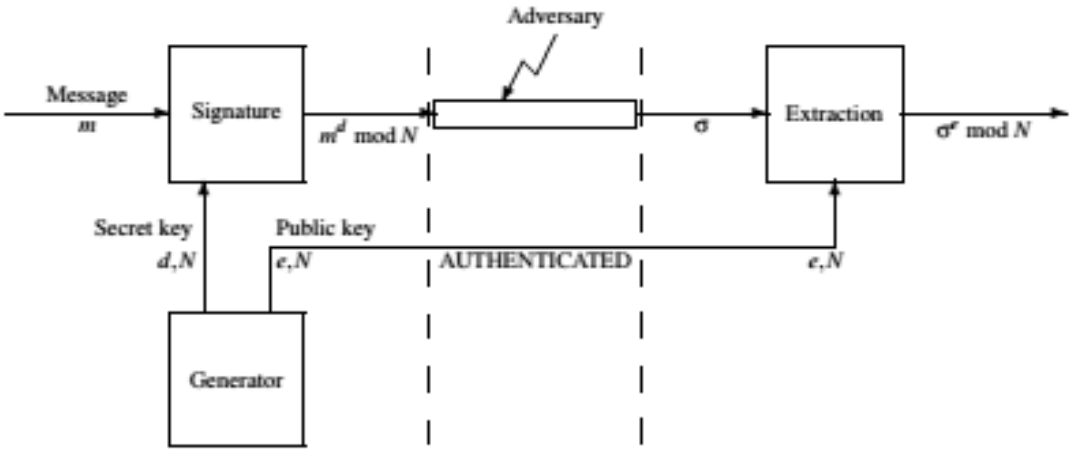
  Έστω ότι K_p = (N, e) και K_s = (N, d) είναι ένα RSAζεύγος κλειδιών για υπογραφή. Η υπογραφή ενός μηνύματος m χρησιμοποιώντας τον απλό

αλγόριθμο RSAείναι σ = m^d, όπως φαίνεται και στο σχήμα 17. Αυτό βέβαια έχει πολλά προβλήματα, που οφείλονται κυρίως στις ιδιότητες του RSA.

Αρχικά, είναι εύκολο για τον οποιονδήποτε να διαλέξει ένα τυχαίο σ και να κατασκευάσει το σ = m^dmodN, που δημιουργεί ένα έγκυρο ζεύγος (m, σ). Πρόκειται για ένα existentialforgery, όπου μπορεί να πλαστογραφηθεί ένα έγκυρο ζεύγος, αλλά δεν υπάρχει έλεγχος στην σημασία του πλαστογραφημένου μηνύματος m.

Στη συνέχεια, μπορεί εύκολα να γίνει επεξεργασία δύο έγκυρων ζευγών (m, σ)και (m', σ'), όπως για παράδειγμα να ληφθεί το m'' = mm' modN και σ''= σσ'modN. Τότε το (m'', σ'') είναι ένα νέο έγκυρο ζεύγος.

Τα παραπάνω προβλήματα ασφάλειας που αναφέρθηκαν μπορούν να διορθωθούν χρησιμοποιώντας hashfunctions κρυπτογραφίας.



Σχήμα 17. Απλό σύστημα υπογραφής RSA

- Digital Signature Standard (DSS)

  ToDSSδημοσιεύτηκετο 1994 απότοNationalInstituteofStandardsandTechnology (NIST) πουαποτελείμέροςτουτμήματοςεμπορίου της Αμερικανικής κυβέρνησης. Περιλαμβάνει έναν DigitalSignatureAlgorithm (DSA). Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές RSA είναι ότι, ενώ στο DSA η παραγωγή υπογραφών είναι πιο γρήγορη από την επιβεβαίωσή τους, στο RSA συμβαίνει το αντίθετο. Η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρόλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μια φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα.

  Το DSS έχει ολοκληρωθεί σε πολλά συστήματα ασφαλείας, αν και έχει λάβει πολλές άσχημες κριτικές, όπως η έλλειψη ευελιξίας, η αργή επαλήθευση των υπογραφών, η αδυναμία συνεργασίας με άλλο πρωτόκολλο πιστοποίησης ταυτότητας και τέλος ότι ο αλγόριθμος δεν έχει αποκαλυφθεί.

10.5 Μετάβαση από την Κρυπτογραφία στην Ασφάλεια της Επικοινωνίας

Στην παράγραφο αυτή περιγράφονται τρόποι να κατασκευαστούν εφαρμογές κρυπτογραφίας που θα παρέχουν ασφάλεια στις επικοινωνίες μέσω μερικών απλών παραδειγμάτων. Ο βασικός στόχος είναι να δημιουργηθεί μια έννοια της ασφαλούς συνόδου επικοινωνίας. Ένα παράδειγμα είναι η τεχνολογία Bluetooth.

Η σύνοδος επικοινωνίας ξεκινά συνήθως με peerauthentication, ανταλλαγή των publickeys και συνεχίζει με ένα πρωτόκολλο συμφωνίας των ταυτοποιημένων κλειδιών. Με αυτό τον τρόπο εξασφαλίζεται ότι και οι δύο peers μοιράζονται ένα

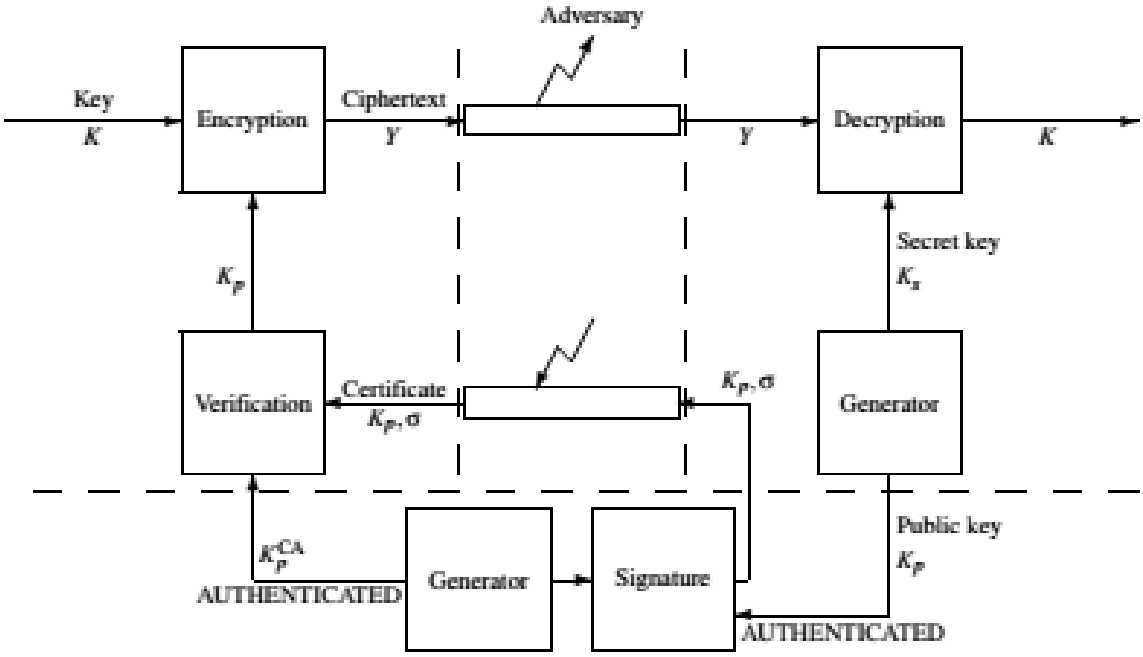
κοινό μυστικό κλειδί. Το μυστικό κλειδί διοχετεύεται σε πολλά συμμετρικά μυστικά κλειδιά. Τότε, η ασφάλεια του μηνύματος, δηλαδή *η ακεραιότητα του μηνύματος*, η *αυθεντικότητα του μηνύματος* και *η εμπιστευτικότητα του μηνύματος*, εξασφαλίζεται μέσω του MAC και της συμμετρικής κρυπτογράφησης. Η ασφάλεια της συνόδου αυτής απαιτεί επιπροσθέτως να εξασφαλιστεί και *η συνέχεια των μηνυμάτων*, πράγμα που σημαίνει ότι κανένας εισβολέας δεν μπορεί να απαντήσει σε ένα μήνυμα, να ανταλλάξει μηνύματα ή να διαγράψει ένα μήνυμα. Αυτό συνήθως εξασφαλίζεται μέσω ενός μετρητή των συγχρονισμένων μηνυμάτων. Μερικές ακόμα ιδιότητες ασφάλειας που μπορεί να απαιτούνται είναι:

- *Χρονοδιαγράμματα παράδοσης των μηνυμάτων* **à** ένας αποστολέας ενός μηνύματος εξασφαλίζει ότι το μήνυμά του θα παραδοθεί στο σωστό παραλήπτη στην ώρα του
- *Δίκαιη διακοπή* **à** οι peers είναι σίγουροι ότι τερματίζουν τη σύνοδο επικοινωνίας βρισκόμενοι στην ίδια κατάσταση
- *Ανωνυμία* **à** ένας peer είναι εξασφαλισμένος ότι δεν θα διαρρεύσει η ταυτότητά του.
- *Μη-εντοπισμός* **à** ένας peer είναι εξασφαλισμένος ότι ο άλλος peer δεν θα μπορεί αργότερα να τον ταυτοποιήσει σε κάποια άλλη σύνοδο επικοινωνίας
- *Μη-διαρροή* **à** οι peers είναι σίγουροι ότι δεν γίνεται αντιληπτό ότι δύο διαφορετικά sessions επικοινωνίας μοιράζονται την ίδια οντότητα.
- *Μη-μεταφορά* **à** ένας peer είναι σίγουρος ότι ο άλλος peer δεν είναι ψεύτικος που κρύβει τον πραγματικό peer, κτλ.

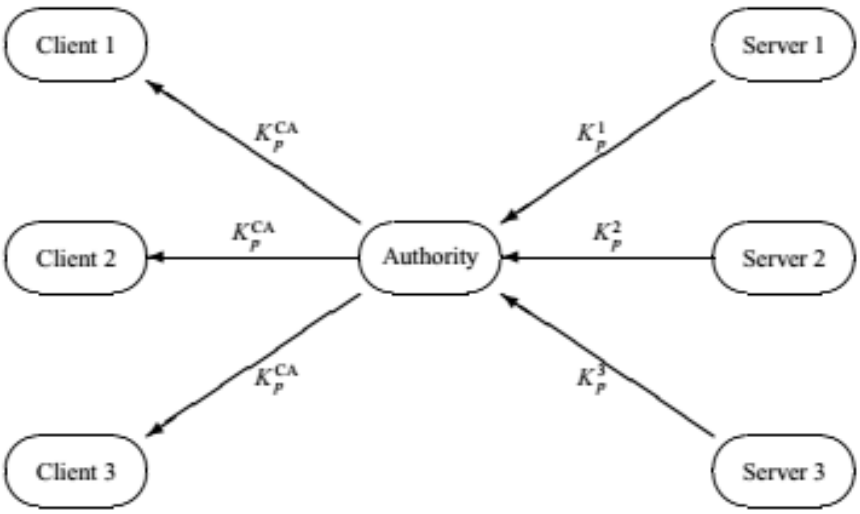
10.5.1 **Πιστοποιητικά**

Η επίτευξη μιας συμφωνίας μυστικού κλειδιού, π.χ. μεταδίδοντας ένα κλειδί Κ χρησιμοποιώντας ένα ασύμμετρο σύστημα κρυπτογραφίας, είναι ένας βολικός τρόπος να γίνει ανταλλαγή ενός πιστοποιημένου μυστικού σε ένα πρωτόκολλο client-server, καθώς μπορεί να χρησιμοποιηθεί αργότερα για να στηθεί ένα

ασφαλές κανάλι επικοινωνίας. Τα πρωτόκολλα συμφωνίας κλειδιών κάνουν τέτοιες υποθέσεις, π.χ. έγινε μετάδοση του publickeyK_p του serverπρος τον client μέσω ενός πιστοποιημένου καναλιού πριν από τη μετάδοση. Το ήδη πιστοποιημένο κανάλι μπορεί να φτιαχτεί από ένα έμπιστο τρίτο μέρος (Σχήμα 18). Πράγματι, ένα certificateauthority (CA) μπορεί να εκδώσει μια υπογραφή σ για K_p και έτσι εγγυάται η πιστοποίηση του publickey. Τα μόνα προβλήματα που απομένουν είναι να εξασφαλιστεί η επικοινωνία του publickeyK_p από τον server προς τοcertificateauthority και η επικοινωνία του authoritypublickeyK_p^{CA}προς τον client (Σχήμα 19).



Σχήμα 18. Ανταλλαγή κλειδιού χρησιμοποιώντας πιστοποιητικά



Σχήμα 19. Κρίσιμα κανάλια ασφαλείας όταν χρησιμοποιούνται πιστοποιητικά

10.5.2 SSH: SecureShell

ΑρχικάτοSSH δημιουργήθηκε για να επιτυγχάνεται απομακρυσμένη πρόσβαση σε έναν υπολογιστή με ασφαλή τρόπο, όταν αυτός χρησιμοποιεί λειτουργικό σύστημα UNIX. Σήμερα υπάρχει μια σειριά από εμπορικές εφαρμογές που βασίζονται στο SSH και ένας πολύ γνωστός ανοιχτός κώδικας που βασίζεται στη βιβλιοθήκη openSSH.

Η βασική αρχή του SSH είναι να υλοποιεί ασφαλή κανάλια επικοινωνίας (έμπιστα και πιστοποιημένα) σε ένα client-serversession. Αρχικά η φιλοσοφία του SSH ήταν να είναι φιλικό προς το χρήστη, χωρίς να απαιτείται κάποια εγκατάσταση για τη χρήση του και να μπορεί να αναπτυχθεί με ευκολία. Παρόλα αυτά, το επίπεδο ασφάλειας δεν ήταν τόσο υψηλό. Η νέα έκδοση του SSH (γνωστή ως SSH2) χρησιμοποιεί δομές public-key για να πιστοποιήσει τους servers. Όταν ένας χρήστης επιθυμεί να συνδεθεί με έναν server, τότε ο server στέλνει το public key μαζί με ένα πιστοποιητικό (αν υπάρχει). Η πρώτη σύνδεση που θα γίνει είναι η πιο κρίσιμη. Εδώ υπάρχουν δύο περιπτώσεις: είτε ο client μπορεί να πιστοποιήσει

ισχυρά το publickey, π.χ. ελέγχοντας ένα πιστοποιητικό ή βάζοντας το χρήστη να ελέγξει το αποτύπωμα του publickey ή ο client θα πρέπει να εμπιστευτεί ότι το publickey είναι σωστό. Στη συνέχεια, ο client αποθηκεύει το publickey σε ένα αρχείο (τυπικά στο .ssh/known_hosts) και υποθέτοντας ότι η πρώτη αυτή σύνδεση είναι επιτυχής, τότε όλες οι μελλοντικές συνδέσεις με τον ίδιο server θα πρέπει να είναι ασφαλείς, αφού θα γίνεται κάθε φορά σύγκριση με το κλειδί που θα λαμβάνεται με το σωστό publickey από αυτό το αρχείο. Η βασική υπόθεση εδώ είναι ότι το αρχείο αυτό θα πρέπει να έχει ασφάλεια ακεραιότητας. Αν τα κλειδιά δεν ταυτίζονται (για οποιοδήποτε λόγο), τότε εμφανίζεται ένα μήνυμα προειδοποίησης στο χρήστη που τον ενημερώνει ότι topublickey έχει αλλάξει και ότι κάποιος εισβολέας ενδεχομένως να προσπαθεί να υποδυθεί τον server στέλνοντας λάθος κλειδί. Τις περισσότερες φορές ο χρήστης δεν ενδιαφέρεται και πατάει OK. Αυτό είναι και το μεγαλύτερο πρόβλημα του SSH.

Στονclientκαιστονserverισχύειέναkeyagreementprotocolτέτοιοώστε ο server είναι πιστοποιημένος και επινοεί ένα συμμετρικό κλειδί που θα χρησιμοποιηθεί για να φτιαχτεί ένα ασφαλές κανάλι. Στη συνέχεια, ο client πιστοποιείται και ταυτοποιείται μέσω ενός κωδικού (password), ο οποίος αποστέλλεται μέσω του ασφαλούς καναλιού.

10.5.3 SSL: SecureSocketLayer

ToSSL είναι ένα ευρέως γνωστό πρωτόκολλο επικοινωνίας που αναπτύχθηκεαρχικά από την Netscape και χρησιμοποιείται στις εφαρμογές του Internet. Το interface είναι παρόμοιο με το TCP/IP με την έννοια ότι οι εφαρμογές που χρειάζεται να επικοινωνήσουν με ασφάλεια ανοίγουν και κλείνουν sockets με παρόμοιο τρόπο. Τα προγράμματα περιήγησης στο Internet χρησιμοποιούν την έκδοση SSL/TLS προκειμένου να επικοινωνήσουν με ασφάλεια με HTTP (HypertextTransferProtocol) servers. Επίσης, μπορεί να χρησιμοποιηθεί και από

άλλες εφαρμογές, όπως π.χ. ένας διαχειριστής email που επιθυμεί να συνδεθεί με τον mailboxserver. Το SSL/TLS είναι σχεδιασμένο έτσι, ώστε να είναι γενικό και να μην βασίζεται σε έναν συγκεκριμένο αλγόριθμο κρυπτογραφίας. Η επιλογή των αλγορίθμων, που λέγεται ciphersuite, καθορίζεται ως σύμβαση ανάμεσα στον clientκαι τον server στην αρχή του session.

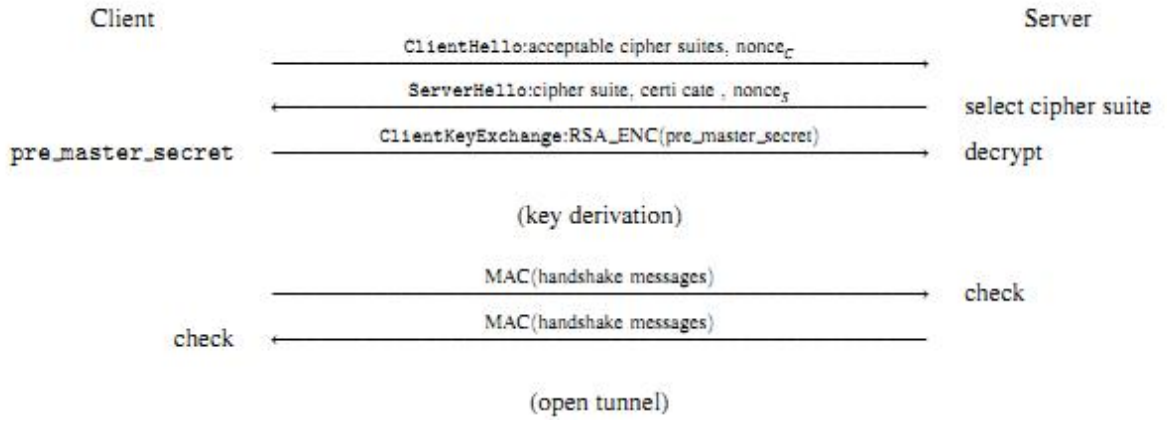
10.5.4 Handshake

Όταν ξεκινά ένα session, τότε ο client και ο server συμφωνούν να χρησιμοποιούν μια έκδοση ενός πρωτοκόλλου, ταυτοποιούν ο ένας τον άλλον προαιρετικά χρησιμοποιώντας πιστοποιητικά και ανταλλάσσουν κλειδιά, όπως περιγράφεται παρακάτω:

1. Ο client στέλνει ένα μήνυμα ClientHello το οποίο περιλαμβάνει το αναγνωριστικό του session, το σετ όλων των ciphersuites που μπορεί να δεχτείκαι ένα nonce (ένας τυχαίος αριθμός που χρησιμοποιείται μόνο σε μια κρυπτογραφημένη επικοινωνία) στον server.
2. Ο server απαντά στέλνοντας ένα μήνυμα ServerHello. Το μήνυμα αυτό περιλαμβάνει το αναγνωριστικό του session, υο ciphersuitepου επέλεξε από το σετ του client και ένα nonce. Συνήθως, στέλνει και το πιστοποιητικό του για να ταυτοποιηθεί. Επίσης, ο server μπορεί να στείλει αίτημα πιστοποίησης, αν επιθυμεί να ταυτοποιήσει τον client
3. Βάσει αυτού, ο client μπορεί να στείλει το πιστοποιητικό του, αν απαιτηθεί από τον server. Επίσης, μπορεί να στείλει ένα μήνυμα ανταλλαγής κλειδιών, ανάλογα με το ποιος αλγόριθμος επιλέχθηκε στην ciphersuite. Αυτό είναι το μήνυμα ClientKeyExhange. Τότε, ο clientκαι ο server μπορούν να υπολογίσουν τέσσερα συμμετρικά κλειδιά: δύο για την κρυπτογράφηση και δύο για το MAC.

4. Ο client στέλνει ένα προστατευόμενο MAC για όλα τα προηγούμενα handshake μηνύματα. Με αυτό τον τρόπο εξασφαλίζεται το γεγονός ότι κανένα μήνυμα δεν θα χαθεί,
5. Με παρόμοιο τρόπο, oserver απαντά με ένα προστατευόμενο MAC για όλα τα προηγούμενα handshake μηνύματα.

Έτσι, ο clientκαι ο server μπορούν να επικοινωνήσουν μέσω ενός προστατευόμενου καναλιού. Ένα τυπικό handshake session απεικονίζεται στο σχήμα 20.



Σχήμα 20. ΈνατυπικόSSL handshake

10.5.5 PGP: Pretty Good Privacy

Σε αντίθεση με το SSL που είναι αφοσιωμένο στην ασφάλεια των on-line επικοινωνιών, το PGP στρέφει το θέμα ασφάλεια σε άλλες έννοιες, όπως η υπογραφή και κρυπτογράφηση των e-mails, των archives κτλ. Το PGP σχεδιάστηκε αρχικά από τον PhilZimmermann στις Ηνωμένες Πολιτείες της Αμερικής κατά τη δεκαετία ’90. Εκείνη την εποχή ήταν σχεδόν παράνομο να εμποδίζεις τις αρχές να έχουν πρόσβαση σε οποιοδήποτε κείμενο μέσω ισχυρής κρυπτογράφησης.

Ορισμένοι, λοιπόν, όπως ο Zimmermann ανέπτυξαν κατάλληλο λογισμικό με σκοπό να παρέχει πρόσβαση στην ισχυρή μυστικότητα για οποιονδήποτε.

Το PGP είναι πολύ εύκολο να εγκατασταθεί και για το λόγο αυτό τα πιστοποιητικά δεν βασίζονται σε καμία αρχή, δεν χρησιμοποιείται καμίαpublic παράμετρος και ο καθένας μπορεί να παράγει ελεύθερα το δικό του κλειδί και να διαλέξει τον αλγόριθμο κρυπτογράφησης. Το PGP μπορεί να χρησιμοποιηθεί για να κρυπτογραφήσει, να απο-κρυπτογραφήσει, να κάνει hash, να υπογράψει ή να πιστοποιήσει ψηφιακά αρχεία ή e-mails. Μερικοί γνωστοί αλγόριθμοι PGP είναι οι IDEAsymmetricencryption, RSAencryptionή υπογραφή και MD5 hashfunction.

Το PGPεπιτρέπει την προστασία μη-διαβασμένων αρχείων (π.χ. κρυπτογραφημένα μηνύματα, υπογραφές, hashedvalues ή ακόμα και κρυπτογραφημένα κλειδιά) κωδικοποιώντας τα σε αναγνώσιμη μορφή. Αυτό γίνεται χρησιμοποιώντας τον Radix-64 code.

Όταν το PGP χρησιμοποιείται για τα e-mail, τότε οι χρήστες μπορούν να δουν ποια έκδοση του PGP χρησιμοποιείται, ποιος αλγόριθμος και ποιο μήκος κλειδιού. Παρακάτω δίνεται ένα παράδειγμα με ένα μήνυμα:

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

PGP makes cryptographic messages readable for human beings.


-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.4 (GNU/Linux)

iD8DBQFBA4c1/LSQdhvwJ58RAjzEAKCXHnwQHNGbX2Bzjo3AMZHABWTW5wCgkx
VLrq22vPs5v1R6RZOf1zEDSF4=
=cVzf
-----END PGP SIGNATURE-----
```

Από το παράδειγμα είναι φανερό ότι η hashedvalue τοy κειμένου σχεδιάστηκε από την GnuPCP.

11 ΑΠΕΙΛΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

11.1 Κακόβουλα προγράμματα

Ως κακόβουλα προγράμματα (malicious software) χαρακτηρίζονται τα προγράμματα που εκτελούν καταστροφικές ενέργειες σε υπολογιστικά συστήματα και προκαλούν ανεπιθύμητα αποτελέσματα, όπως εμφάνιση μηνυμάτων, διαγραφή αρχείων, ακόμη και φορμάρισμα δίσκων.

Ένα μεγάλο πρόβλημα με τα κακόβουλα προγράμματα είναι ότι μπορεί να παραμένουν αδρανή στη μνήμη του υπολογιστή για μεγάλο χρονικό διάστημα. Τα αποτελέσματά τους γίνονται αντιληπτά όταν ενεργοποιούνται μετά από κάποιο συμβάν ή σε μια συγκεκριμένη ημερομηνία. Αυτό όμως που κάνει τα κακόβουλα προγράμματα ιδιαίτερα επικίνδυνα είναι η δυνατότητά τους να αντιγράφονται και να εξαπλώνονται από υπολογιστή σε υπολογιστή.

Οι βασικοί τύποι κακόβουλων προγραμμάτων περιγράφονται στη συνέχεια και είναι:

1. Ιοί Υπολογιστών (Computer Viruses)
2. Δούρειοι Ίπποι (Trojan Horses)
3. Σκουλήκια (Worms)
4. Λογικές Βόμβες (Logic Bombs): κακόβουλα προγράμματα που «εκρήγνυνται» όταν ικανοποιηθεί μια λογική συνθήκη.
5. Χρονικές Βόμβες (Time Bombs): κακόβουλα προγράμματα που ενεργοποιούνται όταν έρθει η κατάλληλη χρονική στιγμή ή μέρα.
6. Πίσω πόρτες (Trapdoors/Backdoors): κρυμμένες λειτουργίες προγραμμάτων με τις οποίες παρέχεται η προσπέλαση σε ευαίσθητα δεδομένα.

7. Κουνέλια (Rabbits): προγράμματα που αυτο-αντιγράφονται απεριόριστα με σκοπό την υπερβολική κατανάλωση υπολογιστικών πόρων.

11.1.1 Ιοί

Ιοί Υπολογιστών (Computer Viruses) ονομάζονται τα μέρη κώδικα που είναι προσαρτημένα σε ένα κανονικό (ωφέλιμο) πρόγραμμα και αντιγράφονται από μόνα τους (self-replicating). Μπορεί να μην κάνουν τίποτε, να μην προκαλούν ζημιές (π.χ. να παίζουν κάποιο τόνο μουσικής) ή να είναι καταστροφικά (π.χ. να μεταβάλλουν και να σβήνουν αρχεία). Υπάρχουν διάφοροι τύποι ιών:

- Ιοί Εκκίνησης (Bootstrap Viruses): κώδικας που εισάγεται στην διαδικασία εκκίνησης ενός υπολογιστή.
- Παρασιτικοί Ιοί (Parasitic Viruses): μέρη κώδικα που προσαρτώνται σε εκτελέσιμα προγράμματα (αρχεία .COM ή .EXE).
- Συνοδευτικοί Ιοί (Companion Viruses): εναλλακτικά εκτελέσιμα προγράμματα που εισάγονται στην διαδρομή αναζήτησης κανονικών προγραμμάτων.
- Ιοί Μακροεντολών (Macro Viruses): τμήματα κώδικα που εισάγονται σε αρχεία δεδομένων τα οποία επεξεργάζεται μια εφαρμογή που υποστηρίζει μακροεντολές.

Το ευτύχημα είναι ότι οι ιοί που εισχωρούν σε ένα σύστημα δεν μπορούν να παραμείνουν ολότελα αόρατοι αφού ο ιοικός κώδικας πρέπει να αποθηκευτεί κάπου. Αυτό σημαίνει ότι ο ιοί μπορούν να ανιχνεύονται με αναζήτηση των χαρακτηριστικών ακολουθιών πληροφοριών που ονομάζονται υπογραφές (signatures).

Παρόλα αυτά οι ιοί μπορούν να κρύβονται (κατά ένα μέρος) είτε τεμαχίζοντας τον κώδικά τους είτε αποθηκευόμενοι σε κρυπτογραφημένη μορφή, όπως οι πολυμορφικοί ιοί (polymorphic viruses), χρησιμοποιώντας ένα μεταβλητό κρυπτογραφικό κλειδί το οποίο επίσης αποθηκεύεται μαζί με τον κρυπτογραφημένο ιοικό κώδικα. Το μέρος όμως του ιοικού κώδικα που είναι υπεύθυνο για την διαδικασία αποκρυπτογράφησης πρέπει να παραμένει χωρίς κρυπτογράφηση, αφήνοντας έτσι μια, έστω μικρή, υπογραφή που είναι ικανή για τον εντοπισμό των πολυμορφικών ιών.

Όσον αφορά τον τρόπο ενεργοποίησής τους, οι ιοί αντιγράφονται από μόνοι τους με δυο βασικούς τρόπους. Όταν εκτελείται ένα μολυσμένο πρόγραμμα:

- είτε μολύνει άμεσα άλλα μέρη του υπολογιστή (transient), π.χ. άλλες τοποθεσίες στο δίσκο ή άλλα προγράμματα
- είτε εγκαθίσταται μόνιμα στη μνήμη (memory resident) από μόνο του και κατόπιν μολύνει άλλα προγράμματα που εκτελούνται ή μέσα αποθήκευσης που εισάγονται για χρήση (π.χ. δισκέτες).

10.1.2 **Δούρειοι Ίπποι**

Οι Δούρειοι Ίπποι (Trojan Horses) είναι προγράμματα με κρυφές λειτουργίες που δεν περιλαμβάνονται στην τεκμηρίωση που τα συνοδεύει. Τα προγράμματα αυτά ονομάσθηκαν έτσι γιατί λειτουργούν όπως το μυθικό άλογο του Τρωικού Πολέμου. Δηλαδή, ενώ επικαλούνται ότι επιτελούν κάποια εργασία, στην πραγματικότητα εκτελούν και/ή μια διαφορετική λειτουργία. Αυτή η λανθάνουσα δραστηριότητα είναι που συνήθως εκτελεί καλυμμένες ενέργειες, όπως η κλοπή των συνθηματικών των χρηστών.

Υπάρχουν Δούρειοι Ίπποι που η εργασία που υποτίθεται ότι προσφέρουν δεν υπάρχει καν. Έτσι, όταν εκτελούνται απλά προχωρούν στην απροκάλυπτη

καταστροφή αρχείων και πόρων του συστήματος. Από την άλλη, υπάρχουν Δούρειοι Ίπποι που λειτουργούν με συγκαλυμμένο τρόπο, έτσι ώστε να επιτελούν την εργασία που επικαλούνται χωρίς να προκαλούν υποψίες. Ως Δούρειοι Ίπποι μπορούν να θεωρηθούν και όσα από τα γνωστά προγράμματα του εμπορίου διαθέτουν λειτουργίες οι οποίες δεν αναφέρονται πουθενά στα εγχειρίδια χρήσης τους, αλλά συνήθως αποκαλύπτονται τυχαία.

Είναι προφανές ότι οι Δούρειοι Ίπποι αποτελούν την πλέον επικίνδυνη κατηγορία κακόβουλων προγραμμάτων, καθώς φανερά επικαλούνται μια δεδομένη λειτουργικότητα ενώ στην πραγματικότητα λειτουργούν λίγο ή πολύ διαφορετικά και μάλιστα χωρίς αυτό να φαίνεται. Έτσι, δεν χρειάζεται να αντιγράφουν τους εαυτούς τους ούτε να αναπαράγονται όπως οι ιοί και τα σκουλήκια. Είναι οι ίδιοι οι χρήστες που βοηθούν τους Δούρειους Ίππους να μολύνουν τα διάφορα υπολογιστικά συστήματα.

Κύριες πηγές Δούρειων Ίππων είναι οι διάφοροι εξυπηρετητές πληροφόρησης (bulletin board servers) και διανομής αρχείων (FTP servers). Σε αυτούς τους τόπους κανείς μπορεί να βρει πληθώρα ελεύθερων (freeware,shareware,demos) και πολλές φορές πειρατικών αντιγράφων προγραμμάτων τα οποία διατίθενται για ‘κατέβασμα’(download) με μικρή ή καθόλου εγγύηση. Φυσικά με κίνητρο την δωρεάν απόκτηση «χρήσιμου» λογισμικού, οι χρήστες αναλαμβάνουν το ρίσκο να γίνουν οι ίδιοι βοηθοί των συγγραφέων των Δούρειων Ίππων, εγκαθιστώντας τους στους υπολογιστές τους.

Οι πιο χρήσιμοι Δούρειοι ίπποι ονομάζονται πίσω πόρτες. Αυτά τα προγράμματα παρέχουν ένα μηχανισμό με βάση τον οποίο ο εισβολέας μπορεί να ελέγξει απευθείας τον υπολογιστή. Παραδείγματα περιλαμβάνουν κακόβουλα σχεδιασμένα προγράμματα όπως τα NetBus, Back Orifice και BO2K, καθώς και καλοκάγαθα προγράμματα, τα οποία μπορεί να εκμεταλλευθεί κάποιος για να πάρει τον έλεγχο ενός συστήματος, όπως τα netcat, VNC και pcAnywhere. Τα ιδανικά προγράμματα

πίσω πόρτας είναι μικρά και γρήγορα εγκαθιστάμενα προγράμματα, τα οποία εκτελούνται διαρκώς. Οι Δούρειοι ίπποι συνήθως μεταφέρονται μέσω ιών που παράγονται από e-mail ή στέλνονται ως συνημμένα σε e-mail.

Η καλύτερη μέθοδος πρόληψης κατά των Δούρειων Ίππων είναι η ενημέρωση των χρηστών. Σε κάθε περίπτωση όμως είναι δύσκολη αλλά όχι αδύνατη η ανίχνευση των Δούρειων Ίππων πριν να εισχωρήσουν σε ένα υπολογιστικό σύστημα. Για αυτό επιβάλλεται η καθιέρωση και η συνεπής εφαρμογή από τους διάφορους οργανισμούς συγκεκριμένων πολιτικών εγκατάστασης επίσημα αγορασμένου λογισμικού, καθώς και εκπαίδευσης των χρηστών, έτσι ώστε να αποκτήσουν τα απαραίτητα για να συμμερίζονται τους κινδύνους που αναλαμβάνουν όταν δοκιμάζουν προγράμματα άγνωστης προέλευσης.

10.1.3 **Σκουλήκια**

Τα σκουλήκια (worms) είναι προγράμματα που εξαπλώνονται μέσω των δικτυωμένων υπολογιστών, αντιγράφοντας τα ίδια ανεξέλεγκτα, αλλά συνήθως δεν προκαλούν άλλου τύπου επιπλοκές. Τα σκουλήκια μοιάζουν πολύ με τους ιούς στο ότι αντιγράφονται από μόνα τους και επιτίθενται σε συστήματα με σκοπό να επιφέρουν βλάβες. Πρόκειται για αυτόνομα προγράμματα τα οποία μολύνουν υπολογιστικά συστήματα μόνο μέσω δικτυακών συνδέσεων. Για τη δημιουργία τους απαιτούνται ιδιαίτερες γνώσεις πρωτοκόλλων επικοινωνιών, ευπαθειών δικτυακών συστημάτων και ειδικών θεμάτων πάνω σε λειτουργικά συστήματα.

Μόλις ένα σκουλήκι μολύνει ένα σύστημα, αναζητεί δραστήρια για πιθανές συνδέσεις με άλλους υπολογιστές, οπότε αν βρει, αμέσως αντιγράφεται σε αυτούς. Όμως, πέρα από την συμπεριφορά αναπαραγωγής τους από σύστημα σε σύστημα, τα σκουλήκια συχνά εκτελούν και κακόβουλες πράξεις, που δεν περιορίζονται μόνο στην καταστροφή αρχείων. Έτσι, μέσω των δικτυακών συνδέσεων μπορούν να υποκλέψουν και να μεταφέρουν προς τους συγγραφείς τους πληροφορίες που

αφορούν συνθηματικά χρηστών και άλλες ευαίσθητες αλλά και πολύτιμες πληροφορίες. Επιπλέον, μπορούν να επιφέρουν πλήρη αποδιοργάνωση των λειτουργιών ενός συστήματος ώστε να προκαλείται επίθεση άρνησης εξυπηρέτησης (denial of service). Αυτό συνήθως προκαλείται από παράλληλες και ανοργάνωτες επιθέσεις περισσότερων του ενός σκουληκιών στο ίδιο σύστημα.

Ακριβώς επειδή η μόλυνση από σκουλήκια επιτυγχάνεται μέσω δικτυακών συνδέσεων, είναι δύσκολος ο εντοπισμός των σημείων προσβολής. Για την αποφυγή της μόλυνσης από σκουλήκια επιβάλλεται ο εντοπισμός και η αντιμετώπιση όλων των ευπαθών σημείων του υπολογιστικού συστήματος από τους διαχειριστές του. Αυτό σημαίνει ότι ιδιαίτερα πρέπει να προσεχθούν τα αδύνατα σημεία όπως εύκολα συνθηματικά ή ανεξέλεγκτες δικτυακές υπηρεσίες που μπορούν να εκμεταλλευθούν τα σκουλήκια για να εισβάλλουν στο σύστημα από το δίκτυο και να το μολύνουν.

Ένας καλός τρόπος προφύλαξης από τα σκουλήκια είναι η γνώση των μεθόδων που χρησιμοποιούν για τον εντοπισμό και την αξιοποίηση των ευπαθών σημείων του συστήματος. Όπως γίνεται γενικότερα για την πρόληψη εισβολών (intrusion prevention), η χρήση διατάξεων firewalls και ελέγχου προσπέλασης μπορούν να μειώσουν σημαντικά τους κινδύνους επίτευξης των στόχων των σκουληκιών.

11.2 Phishing

Οι όροι phishing και pharming είναι δύο από τα πιο οργανωμένα εγκλήματα του 21ου αιώνα, αφού απαιτούν πολύ λίγη επιδεξιότητα από την πλευρά του ο απατεώνα. Αυτά έχουν ως αποτέλεσμα την κλοπή ταυτότητας του χρήστη και την οικονομική απάτη, καθώς ο απατεώνας εξαπατά τους χρήστες για να αποκαλύψουν εμπιστευτικές τους πληροφορίες, όπως κωδικούς πρόσβασης, αριθμούς κοινωνικής ασφάλισης, πιστωτικές κάρτες Αριθμοί, CVV αριθμούς, και προσωπικές πληροφορίες όπως ημερομηνίες γέννησης και ονόματα των μητέρων κλπ. Οι

πληροφορίες αυτές στη συνέχεια είτε χρησιμοποιείται από απατεώνες για τις δικές τους ανάγκες, όπως η μίμηση του θύματος για να μεταφέρει χρήματα από τον λογαριασμό του θύματος, αγορά εμπορευμάτων κ.λπ., ή πωλείται σε μια ποικιλία από διαδικτυακά φόρουμ διαμεσολάβησης και chat κανάλια με σκοπό το κέρδος.

Η Anti-Phishing Ομάδα Εργασίας (APWG) δημοσίευσε μελέτη, σύμφωνα με την οποία 26.877 επιθέσεις phishing αναφέρθηκαν τον Οκτώβριο του 2006, με 21% αύξηση σχετικά με τις 22.136 επιθέσεις του Σεπτεμβρίου και η αύξηση του 70%, σε σύγκριση με τον Οκτώβριο του 2005. Μέσα από αυτές τις επιθέσεις οι απατεώνες επιτέθηκαν σε 176 επώνυμες μάρκες με αποτέλεσμα τεράστιες οικονομικές απώλειες και την απώλεια της φήμης των επιχειρήσεων. Η μελέτη ανέφερε ότι πάνω από 2 εκατομμύρια Αμερικανοί έχασαν τον έλεγχο των λογαριασμών τους όταν δέχτηκαν επίθεση από εγκληματίες το 2004, ενώ η μέση απώλεια ανά περιστατικό είναι $ 1200.

Η σημερινή τάση των απατεώνων είναι να αναπτύσσουν ακόμα πιο επιδέξιους τρόπους επίθεσης, τείνοντας να αυξήσουν τον αριθμό των επιθέσεων στο εγγύς μέλλον. Συνεπώς, η αντιμετώπιση αυτών των επιθέσεων έχει γίνει υψηλής σημασίας και προτεραιότητας για τις κυβερνήσεις και τη βιομηχανία.

Το phishing είναι κοινωνικός τύπος επίθεσης και ταυτόχρονα τεχνική εξαπάτηση. Οι επιθέσεις κοινωνικού τύπου χρησιμοποιούν πλαστά email για να καθοδηγήσουν τους χρήστες σε ψεύτικες ιστοσελίδες, οι οποίες έχουν σχεδιαστεί για να τους εξαπατήσουν, υποκλέπτοντας τις προσωπικές τους πληροφορίες. Επιπλέον, οι τεχνικές απάτες «φυτεύουν» μολυσμένο λογισμικό (malware), π.χ. ιούς, Trojans κτλ στους υπολογιστές των χρηστών με σκοπό την κλοπή των πληροφοριών τους. Αυτό γίνεται συνήθως με λήψη στιγμιότυπων της οθόνης για την κλοπή των προσωπικών λεπτομερειών.

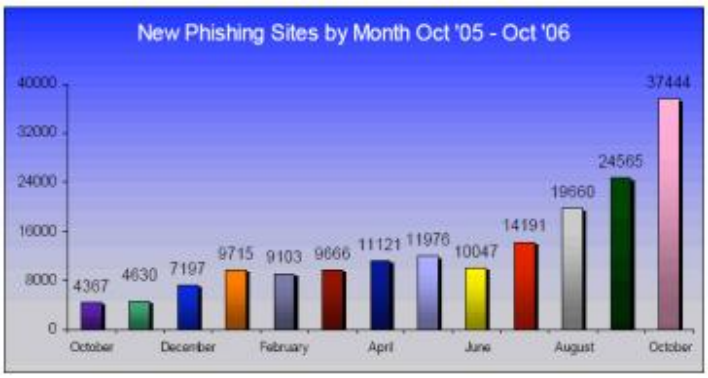
Οι κοινωνικοί τρόποι επίθεσης είναι η πιο συχνή μέθοδος που γίνεται το phishing με email. Το παρακάτω σχήμα 21 παρουσιάζει τον αριθμό των μεμονωμένων αναφορών για καθαρά phishing περιστατικών που καταγράφηκαν από την APWG τον Οκτώβριο του 2006.

Σχήμα 21.

11.2.1 **Εξέλιξη των επιθέσεων** phishing

Ο όρος phishing χρησιμοποιήθηκε στην κλοπή του λογαριασμού AOL, που έγινε με χρήση άμεσου μηνύματος. Εντούτοις, σήμερα ο πιο συχνός τρόπος που χρησιμοποιείται από τους phishers είναι τα email. Επίσης, αυτό που ξεκίνησε ως ένας τρόπος πτωχής γραφής των email που αποστέλλονταν στους χρήστες, σήμερα το phishing έχει εξελιχθεί σε κάτι πολύ πιο δύσκολο να ταυτοποιηθεί, ακόμα και από έναν έμπειρο χρήστη. Τα email τώρα είναι γραμμένα καλύτερα και πιο πειστικά με λίγα ή καθόλου ορθογραφικά λάθη, ενσωματώνοντας τα απαραίτητα λογότυπα και γραφικά. Οι ψεύτικες ιστοσελίδες εξαπάτησης είναι ταυτόσημες στην όψη με αυτές των πραγματικών οργανισμών, καθιστώντας αδύνατη την διαφοροποίησή τους. Αυτή η εικονική αυθεντικότητα έχει ως αποτέλεσμα την αύξηση του αριθμού των νέων ιστοσελίδων phishing κατά το τελευταίο χρονικό διάστημα. Επίσης, η

ευκολία να πραγματοποιηθεί το Phishing το κάνει ένα από τα πιο καλά οργανωμένα δικτυακά εγκλήματα, όπως φαίνεται και στο σχήμα 22.



Σχήμα 22.

11.2.2 **Κίνητρα για** phishing

Το πιο συνηθισμένο κίνητρο πίσω από τις επιθέσεις phishing είναι οικονομικό. Ακόμα και αν ένα μικρό ποσοστό των χρηστών που θα λάβουν το email επίθεσης, δώσει τις εμπιστευτικές του λεπτομέρειες, όπως ονόματα χρηστών, κωδικούς κτλ., η επίθεση θεωρείται μια τεράστια επιτυχία. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν από τους phishers για προσωπικό κέρδος ή να πουληθούν δικτυακά με τεράστιο κέρδος.

11.2.3 **Προσωποποιημένο** phishing

Σε αντίθεση με τις τυπικές επιθέσεις phishing, όπου οι απατεώνες στέλνουν χιλιάδες email σε τυχαίες διευθύνσεις email, στο προσωποποιημένο phishing επιλέγεται μια επιχείρηση με την οποία το πιθανό θύμα συναναστρέφεται οικονομικά, όπως μια τράπεζα ή ένα οικονομικό ίδρυμα ή μια εταιρία πιστωτικών καρτών. Οι απατεώνες ενημερώνουν τον παραλήπτη του email ότι θα πρέπει να «ανανεώσουν» ή να «επαληθεύσουν» τις λεπτομέρειες της πιστωτικής τους κάρτας

ή τις πληροφορίες του λογαριασμού τους έτσι ώστε οι λογαριασμοί τους να παραμείνουν ενεργοί. Για να οργανώσουν το δόλωμα και να μοιάζουν όλα αυθεντικά, κατευθύνουν τα θύματα σε μια ιστοσελίδα που μιμείται το ύφος και την όψη των πραγματικών ιστοσελίδων των οργανισμών που προσποιούνται – με τα ίδια γραφικά, τους ίδιους συνδυασμούς χρωμάτων κτλ. Οι ανυποψίαστοι χρήστες δίνουν τις προσωπικές τους πληροφορίες στους απατεώνες και έτσι πραγματοποιείται η απάτη.

Παράλληλα με τη δημιουργία των ψεύτικων ιστοσελίδων, οι phishers χρησιμοποιούν και τις τελευταίες τεχνολογίες, όπως spyware, keyloggers, mouseloggers και λήψεις εικόνων από τις οθόνες σε μια προσπάθεια να υποκλέψουν τα δεδομένα των χρηστών. Για να ολοκληρωθούν με επιτυχία αυτές οι τεχνικές, θα πρέπει να εκτελεστούν μολυσμένα προγράμματα στον υπολογιστή του θύματος. Αυτά τα προγράμματα μεταβιβάζονται στους χρήστες μέσω καναλιών επικοινωνίας, όπως:

- internet messenger (Yahoo, MSN, κτλ)
- worms/ιούς βασισμένα σε emails

11.2.4 **Άλλοι τρόποι επίθεσης** phishing

Σε άλλους τρόπους phishing επιθέσεων, ένα λάθος στα URL έχει βρεθεί κατά τη διαχείριση του InternationalizedDomainNames (IDN) στους webbrowsers. Αυτό το λάθος, γνωστό ως IDNspoofing, μπορεί να επιτρέπει σε φαινομενικά ταυτόσημες διευθύνσεις να οδηγούν σε άλλες πλαστές, πιθανώς μολυσμένες ιστοσελίδες.

Επιπλέον, το SMiShing είναι μια άλλη μέθοδος επίθεσης, όπου κάποιοι χρήστες κινητών τηλεφώνων λαμβάνουν μηνύματα που τους καλούν να επισκεφθούν διάφορες ιστοσελίδες με ψεύτικες επιβεβαιώσεις για τη σύνδεση σε διάφορες

υπηρεσίες. Αυτή η περίπτωση του phishing μέσω SMS αποδεικνύει ότι οι phishers μέσω κινητών τηλεφώνων αυξάνονται.

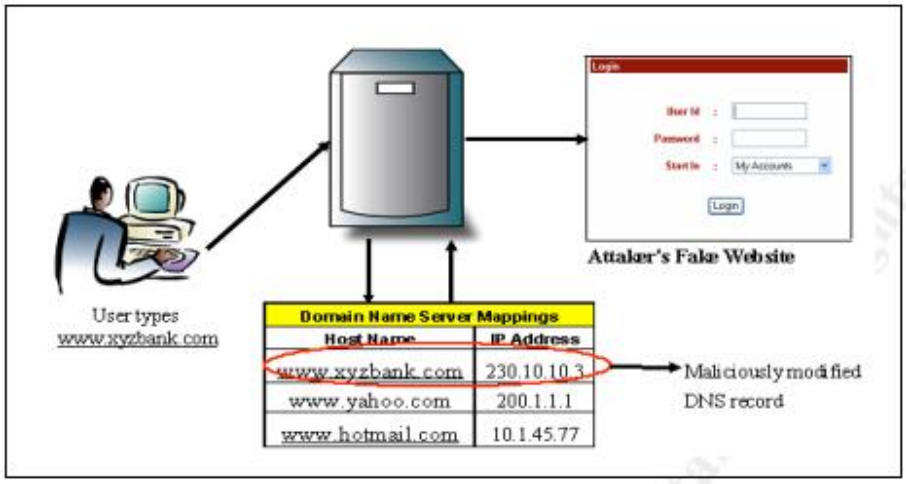
11.3 Pharming

Το pharming είναι μια παρεμφερής διαδικασία με το Phishing, αλλά δεν βασίζεται μόνο στην αποστολή emails σε χιλιάδες χρήστες του διαδικτύου με σκοπό να τους παγιδεύσει. Αυτό που καθιστά το pharming επικίνδυνο είναι το γεγονός ότι η επίθεση δεν μπορεί να ανιχνευθεί και να αναγνωριστεί ούτε από έναν υποψιασμένο χρήστη. Το pharming αξιοποιεί μολυσμένο κώδικα, όπως ιούς, worms, Trojans και spyware για να κάνει εξειδικευμένες επιθέσεις, όπως hostfilemodification, DNScachepoisoning κτλ. Οι pharmers μπορούν να παγιδεύσουν domains με σκοπό να εξαπατήσουν τους χρήστες, κατευθύνοντάς τους σε μολυσμένες ιστοσελίδες.

11.3.1 **Ανατομία μιας επίθεσης** pharming

Η πιο συχνή μέθοδος μιας επίθεσης pharming περιγράφεται παρακάτω (Σχήμα 23):

- Ο χρήστης πληκτρολογεί τη διεύθυνση της τράπεζάς του (π.χ. www.xyzbank.com) στη μπάρα διεύθυνσης του browser.
- Η αίτηση του χρήστη περνά σε ένα DNSnameserver. Αυτός ο διακομιστής αντιστοιχεί το www.xyzbank.com με έναν αριθμό, π.χ. 210.10.19.3, που λέγεται διεύθυνση IP, η οποία είναι κατανοητή από έναν υπολογιστή.
- Σε ένα πραγματικό σενάριο, ο περιηγητής (browser) θα συνδέσει το χρήστη με τη σελίδα επιβεβαίωσης της τράπεζας xyzbank. Εντούτοις, κατά το pharming, ο επιτιθέμενος διαφοροποιεί την προηγούμενη αντιστοιχία στην υπηρεσία DNS. Τώρα, η διεύθυνση www.xyzbank.com αντιστοιχίζεται στο 230.10.10.3 – τη διεύθυνση IP σε μια πλαστή σελίδα του pharmer.



Σχήμα 23.

11.3.2 **Τεχνικές του** Pharming

Το pharming, όπως προαναφέρθηκε, βασίζεται στην αλλαγή του DNS της ιστοσελίδας της εταιρίας. Υπάρχουν διάφοροι τρόποι για να γίνει αυτό, όπως:

- Host file modification

Τα περισσότερα λειτουργικά συστήματα αποθηκεύουν τα αρχεία τοπικά, πράγμα που περιλαμβάνει την αντιστοίχιση ανάμεσα στο domainname και την αντίστοιχη διεύθυνση IP, π.χ. το www.xyzbank.com αντιστοιχεί στο 210.10.10.3. Οι επιτιθέμενοι μπορούν να επωφεληθούν αυτής της ευαισθησίας του λειτουργικού συστήματος, αλλάζοντας αυτά τα αρχεία με μολυσμένες αντιστοιχίες, π.χ. μπορούν να αντιστοιχίσουν το www.xyzbank.com στο 230.10.10.3, που είναι η διεύθυνση IP ενός μολυσμένου site.

- DNS cache poisoning

Οι διακομιστές DNS, για ένα περιορισμένο χρονικό περιθώριο, τοποθετούν σε κρυφή μνήμη (cache) τις αναζητήσεις που γίνονται από τους χρήστες. Αυτό γίνεται για να επιταχύνει το χρόνο αντίδρασης του υπολογιστή σε συχνά χρησιμοποιούμενα domain, ώστε να βελτιώσουν τη δουλειά του χρήστη. Οι pharmers μολύνουν την DNS μνήμη εισάγοντας μολυσμένο περιεχόμενο, ώστε να κατευθύνουν τους χρήστες σε πλαστό προορισμό, όπου ερωτώνται να ανανεώσουν τις προσωπικές του πληροφορίες, όπως κωδικούς και πιστωτικές κάρτες, αριθμούς ασφάλισης και αριθμούς λογαριασμών.

- Χρήση μολυσμένων προγραμμάτων (malware)

Η χρήση malware έχει αυξηθεί πολύ, με τους pharmers να χρησιμοποιούν ιούς και Trojans στο σύστημα του χρήστη που υποκλέπτουν την αίτηση του χρήστη να επισκεφτεί μια συγκεκριμένη ιστοσελίδα, όπως η www.xyzbank.com και τον κατευθύνει στη σελίδα που έχει δημιουργήσει ο pharmer.

- Domains σε κατάσταση ομηρίας (hijacking)

Ο pharmer μπορεί να δεσμεύσει ή να κλέψει την ιστοσελίδα ενός οργανισμού, με τεχνικές όπως το domainslamming και το domainexpiration, με τις οποίες μπορεί να κατευθύνει όλη τη νόμιμη κίνηση του διαδικτύου σε ένα παράνομο site.

- Spoofing ενός στατικού domain name

Ο pharmer μπορεί να αποπειραθεί να εκμεταλλευτεί κάποια μικρά ορθογραφικά λάθη στα domainnames με σκοπό να κοροϊδέψει τους χρήστες να επισκεφθούν κατά λάθος μια μολυσμένη ιστοσελίδα, π.χ. ο pharmer μπορεί να κατευθύνει λανθασμένα το χρήστη στο xyzbnk.com αντί για το xyzbank.com, που είναι η σελίδα που ήθελε πραγματικά να πάει.

12 ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

12.1 Firewall

Η κυριολεκτική έννοια της λέξης firewall έχει να κάνει με πυρίμαχους τοίχους που εμποδίζουν την εξάπλωση της φωτιάς από δωμάτιο σε δωμάτιο ή μεταξύ διαμερισμάτων. Όταν αναφερόμαστε, όμως, στα δίκτυα υπολογιστών, τότε το firewall είναι μια αναγκαία λύση για την προστασία του δικτύου, μιας και οι συνδέσεις μεταξύ των δικτύων και του διαδικτύου αυξάνονται όλο και περισσότερο.

Οι χρήστες ενός δικτύου που είναι συνδεδεμένο στο Internet είναι πλέον σε θέση να αποκτήσουν επαφή και να επικοινωνήσουν με τον «έξω κόσμο», όπως και το αντίθετο, δηλαδή οι εξωτερικοί χρήστες αποκτούν δυνατότητα πρόσβασης σε αυτό το δίκτυο. Όμως, ο κίνδυνος που υπάρχει όταν ένα δίκτυο συνδέεται στο Internet ολοένα και αυξάνεται. Για τη προστασία, λοιπόν, των δικτύων από διάφορες εισβολές απαιτείται ένας κατάλληλος φράκτης, που ονομάζεται firewall, και πρέπει να είναι ικανός να επεξεργάζεται όλη τη κυκλοφορία μηνυμάτων ανάμεσα σε ένα συγκεκριμένο τοπικό δίκτυο και στο Internet. Στην πραγματικότητα ένα σύστημα firewall ανορθώνει ένα εξωτερικό τοίχο ασφάλειας, οριοθετώντας μια περίμετρο προστασίας. Έτσι προκαλεί ένα σαφή διαχωρισμό ανάμεσα στο προστατευμένο-εσωτερικό δίκτυο ενός οργανισμού το οποίο θεωρείται ασφαλές και έμπιστο και στο εξωτερικό διαδίκτυο το οποίο θεωρείται μη ασφαλές και μη έμπιστο. Ο πρωταρχικός σκοπός των firewalls δηλαδή είναι να προστατεύσουν τα δίκτυα από εξωτερικούς εισβολείς, περιορίζοντας τους τα δικαιώματα προσπέλασης σε αυτό, χωρίς να περιορίζουν την προσπέλαση στον εξωτερικό περιβάλλον.

Ένα σύστημα firewall μπορεί να επιτρέπει επιλεκτικά την πρόσβαση στους εξωτερικούς χρήστες, βασιζόμενο σε ονόματα χρηστών και συνθηματικά ή σε IP διευθύνσεις ή ακόμη και σε ονόματα επικρατειών (domain names). Ο κύριος

σκοπός του δηλαδή είναι να κρατήσει τις επικίνδυνες δραστηριότητες μακριά από το περιβάλλον που προστατεύεται. Είναι χαρακτηριστικό ότι ένα firewall θεωρείται ότι διαθέτει δύο μηχανισμούς, έναν για να εμποδίζει την κυκλοφορία της πληροφορίας και έναν άλλον για να επιτρέπει τη ροή της, βάσει μιας πολιτικής ελέγχου που υιοθετείται. Ένα σύστημα firewall δεν είναι απλά και μόνο ένας δρομολογητής, ένας διανομέας ή διακομιστής, ένας οικοδεσπότης ή ένα σύνολο εξοπλισμού και λογισμικού που παρέχει ασφάλεια στα δίκτυα. Οι αληθινές δυνατότητές του γίνονται εμφανείς αν τον θεωρήσουμε ως ένα ισχυρό μέσο υλοποίησης μιας πολιτικής ασφάλειας που καθορίζει τις παρεχόμενες υπηρεσίες και τις επιτρεπτές προσπελάσεις ανάμεσα σε έμπιστες και μη έμπιστες επικράτειες. Η υλοποίηση της πολιτικής ελέγχου προσπέλασης δικτύων γίνεται με την υποχρεωτική κατεύθυνση όλων των επικοινωνιών μέσω του firewall, ώστε να αποτελούν αντικείμενο για παραπέρα εξέταση και καταγραφή από αυτό.

Μια τυπική διάταξη firewalls παρουσιάζεται στην ακόλουθη εικόνα:

Σχήμα 24. Τυπικό Firewall

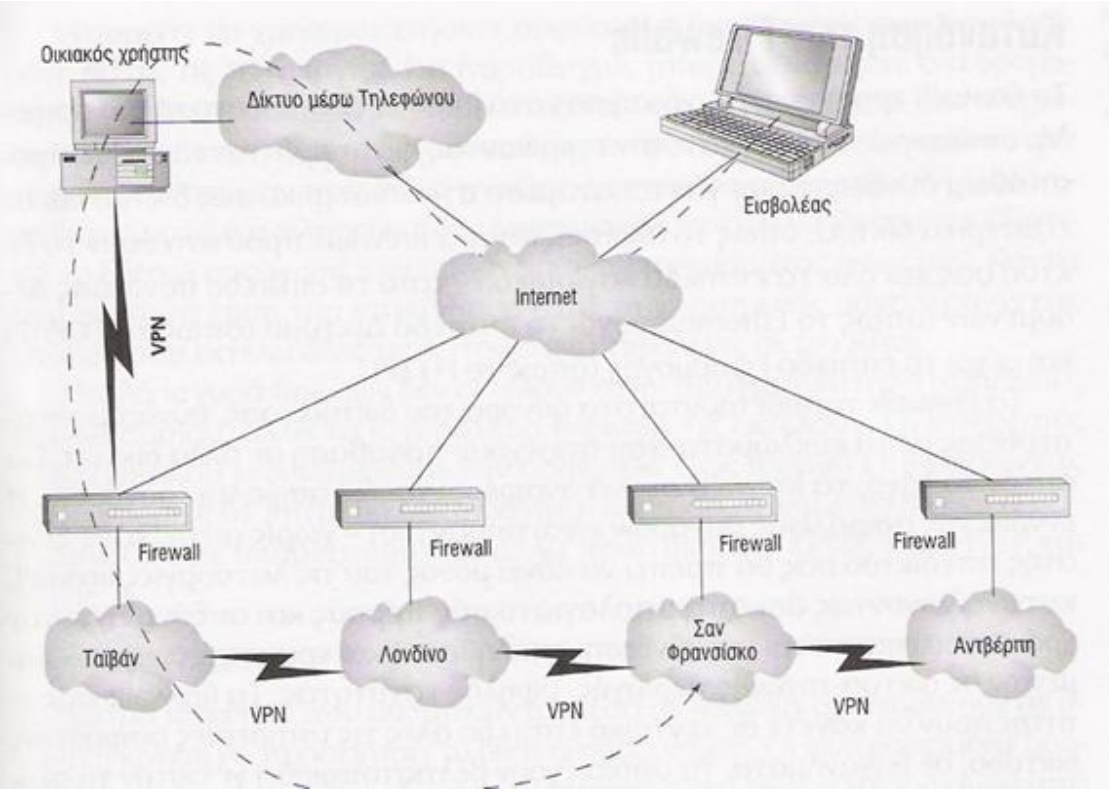
Σε αυτή τη διάταξη, το εσωτερικό δίκτυο χωρίζεται από τα εξωτερικά δίκτυα με μια πύλη firewall. Η πύλη χρησιμοποιείται για την παροχή:

- υπηρεσιών αναμετάδοσης μεταξύ των δικτύων και
- υπηρεσιών φιλτραρίσματος για περιορισμό των πληροφοριών που διέρχονται με προορισμό/αφετηρία τους ξενιστές του εσωτερικού δικτύου.

Τα firewalls κρατούν τη σύνδεση στο Internet όσο το δυνατό πιο ασφαλή, επιθεωρώντας και κατόπιν εγκρίνοντας ή απορρίπτοντας κάθε προσπάθεια σύνδεσης που γίνεται ανάμεσα στο εσωτερικό δίκτυο μιας εταιρείας και σε εξωτερικά δίκτυα, όπως το Internet. Ισχυρά firewalls προστατεύουν ένα δίκτυο υπολογιστών και όλα τα επίπεδα λογισμικού - από το επίπεδο σύνδεσης Δεδομένων όπως το Ethernet μέχρι το επίπεδο Δικτύου όπως το TCP/IP και μέχρι το επίπεδο Εφαρμογής όπως το HTTP.

Τα firewalls τοποθετούνται στα σύνορα του δικτύου, συνδεόμενα απευθείας με τα κυκλώματα που παρέχουν πρόσβαση σε άλλα δίκτυα. Για αυτόν το λόγο, τα firewalls συχνά αναφέρονται ως ασφάλεια συνόρων. Η έννοια της ασφάλειας συνόρων είναι σημαντική αφού χωρίς αυτή, κάθε ξενιστής στο δίκτυο θα πρέπει να κάνει μόνος του τις λειτουργίες firewall, καταναλώνοντας άσκοπα υπολογιστικούς πόρους και αυξάνοντας τον χρόνο που απαιτείται για σύνδεση, επαλήθευση και κρυπτογράφηση δεδομένων σε δίκτυα τοπικής περιοχής, υψηλής ταχύτητας. Τα firewalls επιτρέπουν να γίνονται σε κεντρικό επίπεδο όλες τις υπηρεσίες ασφάλειας δικτύου, σε μηχανήματα, τα οποία έχουν βελτιστοποιηθεί γι' αυτόν το σκοπό και είναι αφοσιωμένα σε αυτήν την εργασία.

Από τη φύση τους, τα firewalls δημιουργούν συνωστισμούς ανάμεσα στο εσωτερικό και στο εξωτερικό δίκτυο, όπως φαίνεται και από το Σχήμα 25 επειδή όλη η κίνηση που κινείται ανάμεσα στο εσωτερικό και στο εξωτερικό δίκτυο πρέπει να περάσει από ένα μόνο σημείο ελέγχου. Αυτό είναι ένα μικρό τίμημα που πρέπει να πληρώσει κανείς για να έχει ασφάλεια. Εφόσον οι εξωτερικές συνδέσεις μισθωμένων γραμμών είναι σχετικά αργές σε σχέση με την ταχύτητα των σύγχρονων υπολογιστών, η υστέρηση που προκαλείται από τα firewalls μπορεί να είναι τελείως διαφανής.



Σχήμα 25: Τοποθέτηση Firewall πίσω από μηχανήματα με εκτεταμένη σύνδεση στο Διαδίκτυο

12.1.1 **Παρεχόμενη Ασφάλεια**

Καθώς τα τοπικά δίκτυα συνδέονται στο Internet, αποτελεί ζήτημα μεγάλης σημασίας η διασφάλιση της κανονικής λειτουργίας τους από τους νόμιμους και παράνομους χρήστες τους. Η τοποθέτηση ενός firewall συστήματος ανάμεσα στο τοπικό δίκτυο μιας επιχείρησης και το διαδίκτυο, παρέχει δυνατότητες ελέγχου στη ροή των πληροφοριών και διασφαλίζει τη σύνδεσή του με το διαδίκτυο, προστατεύοντας εκ μέρους της επιχείρησης τους πόρους της από φθορά, κατάχρηση, ή κλοπή, την υπόληψή της από τη δημοσιοποίηση αδυναμιών στην ασφάλεια του δικτύου της καθώς και την επικρατούσα πολιτική ορθής χρήσης των υπηρεσιών του διαδικτύου από τους εργαζομένους της.

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

Ακόμη, μια επιχείρηση μπορεί να χρησιμοποιήσει ένα firewall για να απομονώσει τις επικοινωνίες ανάμεσα στα δίκτυα των επιμέρους τμημάτων της. Για παράδειγμα ένα νοσοκομείο ενδεχομένως να θελήσει να διαχωρίσει το δίκτυο διακίνησης των δεδομένων των ασθενών από το δίκτυο των οικονομικών στοιχείων του. Ένα ή περισσότερα firewalls μπορούν να χρησιμοποιηθούν για να παρέχουν απομόνωση και ελεγχόμενη προσπέλαση ανάμεσα στα διάφορα μέρη ενός οργανισμού ή μιας επιχείρησης.

Ως ένα σύστημα firewall μπορεί να θεωρηθεί μια διάταξη δρομολόγησης, ένας προσωπικός υπολογιστής, ένας διακομιστής, ή ένα σύνολο από διακομιστές, διαμορφωμένοι με τέτοιο τρόπο ώστε να οχυρώνουν μια δικτυακή τοποθεσία ή ένα υποδίκτυο από πρωτόκολλα και υπηρεσίες, όπως οι υπηρεσίες FTP, HTTP, e-mail, οι οποίες μπορούν να προσβληθούν από διακομιστές εκτός του υποδικτύου. Η συνηθισμένη θέση του είναι ως πύλη υψηλού επιπέδου ακριβώς στο σημείο σύνδεσης της επιχείρησης με το Internet.

Η εγκατάσταση επιπλέον συστημάτων firewall ως διαχωριστικά των επιμέρους τμημάτων μιας επιχείρησης, προσφέρει δυνατότητες διαχωρισμού των εξουσιοδοτήσεων που προσφέρονται στους εσωτερικούς χρήστες, λεπτομερέστερη επίβλεψή τους και γενικότερα υποστήριξη υπευθυνότητας με περισσότερη

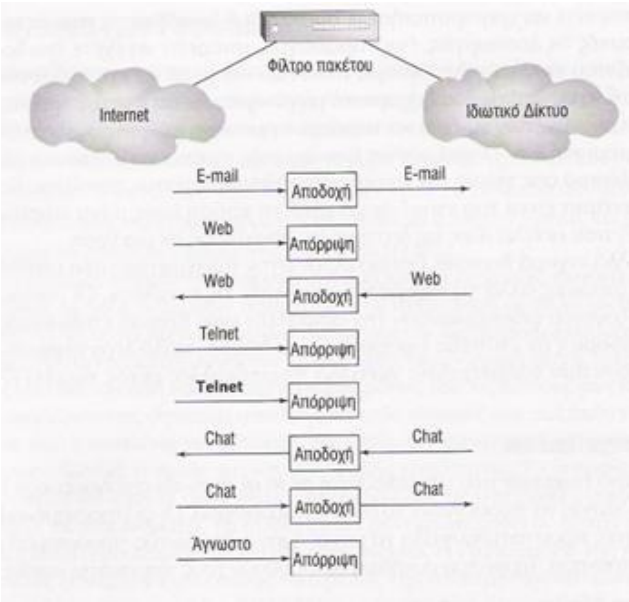
διακριτικότητα. Με άλλα λόγια, **παρέχει μέτρα προστασίας από τους νόμιμους και εσωτερικούς χρήστες του δικτύου, που σύμφωνα και με τις περισσότερες έρευνες αποτελούν τον σημαντικότερο κίνδυνο για την ασφάλεια μιας επιχείρησης**.

12.1.2 **Τεχνικές Ασφαλείας με** Firewalls

Υπάρχουν τέσσερις βασικές τεχνικές προστασίας:

1. *Πύλες φιλτραρίσματος πακέτων (packet filtering gateways) ή δρομολογητές φιλτραρίσματος (screening routers).*

Οι πύλες φιλτραρίσματος πακέτων παρέχουν έναν εύκολο και φθηνό τρόπο υλοποίησης ενός βασικού επιπέδου φιλτραρίσματος με πραγματοποίηση ελέγχων των IP πακέτων ενός δικτύου. Ένα πακέτο είναι μια μικρή μονάδα επικοινωνίας, συνήθως μερικές εκατοντάδες bytes. Ένας δρομολογητής μπορεί να διοχετεύσει χιλιάδες πακέτα μέσα σε ένα δευτερόλεπτο.



Σχήμα 26: Φιλτράρισμα Πακέτων

Το φίλτρο πακέτων, όπως φαίνεται και στο Σχήμα 26, διενεργεί τον έλεγχο εφαρμόζοντας ένα σύνολο κανόνων οι οποίοι έχουν οριστεί από το διαχειριστή του firewall κατά τη διαμόρφωσή του και οι οποίοι υλοποιούν μια προαποφασισμένη πολιτική ασφάλειας. Κάθε κανόνας έχει δυο βασικά τμήματα το πεδίο της ενέργειας και το πεδίο των κριτηρίων επιλογής. Οι δυνατές ενέργειες είναι δύο, επιτρέπω ή σταματώ. Τα κριτήρια επιλογής των πακέτων για τα οποία θα ισχύσει η αντίστοιχη ενέργεια, βασίζονται στην διεύθυνση προέλευσης και προορισμού των πακέτων, στον αριθμό θυρίδας προέλευσης και προορισμού, στο πρωτόκολλο, αν είναι για παράδειγμα TCP (Transmission Control Protocol), ICMP (Internet Control Message Protocol) ή UDP (User Datagram Protocol) καθώς και στην κατεύθυνση, δηλαδή στο αν εισέρχεται το πακέτο στο ιδιωτικό δίκτυο ή αν εξέρχεται από αυτό.

Σε γενικές γραμμές το επίπεδο ασφάλειας που προσφέρουν είναι χαμηλού επιπέδου. Από την άλλη μεριά πάλι, είναι ευέλικτοι, απλοί, γρήγοροι, και χαμηλού κόστους. Έτσι θεωρούνται ιδανικοί για περιβάλλοντα χαμηλής επικινδυνότητας. Βεβαίως οι υπηρεσίες που προσφέρουν είναι σημαντικότατες για αυτό και θεωρούνται αναπόσπαστο τμήμα ενός ολοκληρωμένου συστήματος firewall.

2. *Πύλες κυκλωμάτων (circuit gateways)*

Η χρήση των πυλών κυκλωμάτων σε διατάξεις firewalls αναβαθμίζει σημαντικά την ασφάλεια των δικτύων. Επιτρέπουν τη χρήση εφαρμογών που βασίζονται στα πρωτόκολλα επικοινωνίας TCP και UDP, όπως για παράδειγμα WWW και Telnet χωρίς να αφήνουν να γίνονται όλα σε επίπεδο πρωτοκόλλου επικοινωνίας.

Οι πύλες κυκλωμάτων λειτουργούν ως εκπρόσωποι των πρωτοκόλλων επικοινωνίας, μεταβιβάζοντας την δικτυακή κίνηση μεταξύ δυο υπολογιστών που είναι συνδεδεμένοι μεταξύ τους μέσω ενός ιδεατού κυκλώματος του δικτύου. Ένας εσωτερικός χρήστης, για παράδειγμα, μπορεί να συνδέεται σε μια θύρα της πύλης η

οποία στη συνέχεια μπορεί να συνδέεται σε μια άλλη θύρα ενός υπολογιστή που βρίσκεται σε ένα εξωτερικό δίκτυο. Η πύλη απλά αντιγράφει bytes από την μια θύρα στην άλλη. Κανονικά η πύλη μεταβιβάζει τα δεδομένα χωρίς να τα εξετάζει, αλλά συνήθως διατηρεί μια καταγραφή της ποσότητας των μεταβιβαζόμενων δεδομένων και του προορισμού τους. Σε μερικές περιπτώσεις η σύνδεση μεταβίβασης, η οποία με αυτό τον τρόπο διαμορφώνει τελικά ένα 'κύκλωμα', λειτουργεί αυτόματα. Άλλες φορές πάλι, χρειάζεται να καθορισθεί στην πύλη η επιθυμητή θύρα προορισμού.

Ένα από τα μειονεκτήματα αυτών των συστημάτων είναι ότι οι εφαρμογές των πελατών πρέπει να μετατραπούν πριν να καταστούν έτοιμες για να λειτουργήσουν με μια συγκεκριμένη πύλη κυκλωμάτων.

3. *Πύλες εφαρμογών (application gateways)*

Οι πύλες κυκλωμάτων και οι πύλες εφαρμογών αναφέρονται και ως proxy servers, καθώς και οι δυο συμπεριφέρονται ως εκπρόσωποι του υποτιθέμενου πελάτη. Όμως οι πύλες εφαρμογών προχωρούν ακόμη παραπέρα, σε ότι αφορά την ασφάλεια των δικτύων. Λειτουργούν στο υψηλότερο στρώμα επικοινωνίας, γνωστό ως το επίπεδο εφαρμογής. Έτσι έχουν πρόσβαση σε περισσότερες πληροφορίες από ότι τα συστήματα με απλό φιλτράρισμα πακέτων και μπορούν να προγραμματιστούν πιο έξυπνα κάνοντάς τα ικανά να υποστηρίξουν σύνθετες πολιτικές ασφάλειας.

Όλα τα IP-πακέτα που φτάνουν ή που πρέπει να φύγουν, εξετάζονται πρώτα ως προς το περιεχόμενό τους και ανάλογα προωθούνται ή απορρίπτονται. Για το σκοπό αυτό χρησιμοποιούνται προγράμματα που εκτελούνται ως εφαρμογές, οι οποίες ονομάζονται proxies. Κάθε TCP/IP υπηρεσία που θέλουμε να ελέγχεται από το firewall, έχει το δικό της proxy, δηλαδή μια υπηρεσία διαμεσολαβητή. Για

παράδειγμα, ένας χρήστης προερχόμενος από το Internet, για να αποκτήσει πρόσβαση στην υπηρεσία FTP ενός μηχανήματος του προστατευμένου δικτύου, θα πρέπει πρώτα να συνδεθεί με τη αντίστοιχη proxy εφαρμογή, να ακολουθήσει η αναγνώριση - πιστοποίησή του και στη συνέχεια, αν η πολιτική ασφάλειας του firewall περιέχει για το συγκεκριμένο και αναγνωρισμένο χρήστη τις κατάλληλες εξουσιοδοτήσεις, θα προωθηθεί η σύνδεση με την υπηρεσία FTP που ζήτησε.

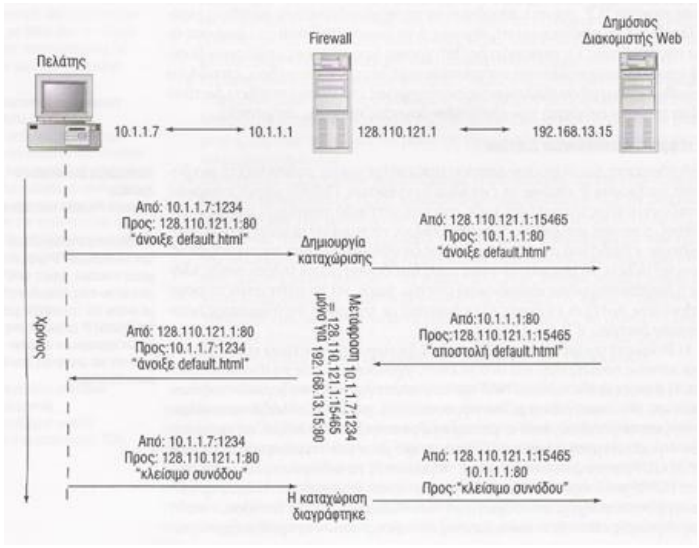
Στην πραγματικότητα, δηλαδή, ένα τέτοιου τύπου firewall ή συστατικό ενός firewall, εκτελώντας ψευδοεφαρμογές, παρεμβάλλεται μεταξύ των πρωτοκόλλων επικοινωνίας προκειμένου να ελέγχει τη νομιμότητα των επικοινωνιών. Καμιά άλλη υπηρεσία δεν μπορεί απευθείας να στείλει ή να λάβει δεδομένα. Αυτός είναι άλλωστε και ο ρόλος του συστήματος firewall, να λειτουργεί δηλαδή ως ένα ισχυρό τείχος ασφαλείας αλλά και ικανό να προσαρμόζεται εύκολα στις ανάγκες επικοινωνίας ενός δικτύου. Η τεχνολογία αυτή προσφέρει ολοκληρωμένη ασφάλεια με τους ισχυρούς μηχανισμούς αυθεντικοποίησης χρηστών και συστημάτων, καταγραφής και υποστήριξης υπευθυνότητας που διαθέτει.

4. *Πύλες μετάφρασης διευθύνσεων Δικτύου*

Η Μετάφραση Διευθύνσεων Δικτύου επιτρέπει την πολύπλεξη μιας δημόσιας διεύθυνσης IP επάνω σε ένα ολόκληρο δίκτυο. Πολλές μικρές εταιρείες βασίζονται στις υπηρεσίες ενός παρόχου υπηρεσιών Internet, ο οποίος μπορεί να είναι απρόθυμος να παρέχει μεγάλα μπλοκ διευθύνσεων, επειδή και ο δικός του χώρος διευθύνσεων είναι περιορισμένος. Ίσως να υπάρχει όμως η ανάγκη κάποιος χρήστης να μοιραστεί μια μόνο διεύθυνση μέσω τηλεφωνικής κλήσης ή διεύθυνσης μέσω καλωδιακού μόντεμ, χωρίς να ενημερώσει για αυτό τον πάροχο υπηρεσιών. Αυτές οι επιλογές είναι δυνατές με τη χρήση Μετάφρασης Διευθύνσεων Δικτύου.

Το NAT αρχικά αναπτύχθηκε επειδή ήταν δύσκολο να πάρει ένας χρήστης και ακόμα περισσότερο μια επιχείρηση με κάποιο δίκτυο υπολογιστών, μεγάλα μπλοκ δημόσιων διευθύνσεων IP και τα δίκτυα συχνά εξαντλούσαν την εκχωρημένη τους δεξαμενή πριν να μπορέσουν να ζητήσουν περισσότερες διευθύνσεις από το InterNIC. Το InterNIC άρχισε να εξοικονομεί διευθύνσεις, όταν άρχισε η επανάσταση του Internet, επειδή η δεξαμενή των διαθέσιμων διευθύνσεων εξαντλήθηκε γρήγορα. Πολυπλέκοντας μια μόνο δημόσια διεύθυνση με αρκετούς εσωτερικούς ξενιστές μέσα σε μια ιδιωτική περιοχή IP, μια εταιρεία μπορούσε να έχει μόνο μια δημόσια διεύθυνση IP.

Το NAT κρύβει τις εσωτερικές διευθύνσεις IP, μετατρέποντας όλες τις εσωτερικές διευθύνσεις ξενιστών στη δημόσια διεύθυνση του firewall. Το firewall κατόπιν μεταφράζει τη διεύθυνση του εσωτερικού ξενιστή από την δική του διεύθυνση, χρησιμοποιώντας τον αριθμό θύρας TCP για να παρακολουθεί ποιες συνδέσεις στη δημόσια πλευρά αντιστοιχούν με ποιους ξενιστές στην ιδιωτική πλευρά. Για το Internet, όλη η κίνηση στο δίκτυο φαίνεται να προέρχεται από έναν εξαιρετικά απασχολημένο υπολογιστή.



Σχήμα 27: Μετάφραση Διευθύνσεων Δικτύου

Το NAT αποτελεί επίσης πρόβλημα για διαχειριστές δικτύων, οι οποίοι θέλουν να συνδεθούν σε πελάτες πίσω από το διακομιστή NAT για διαχειριστικούς λόγους. Επειδή ο διακομιστής NAT έχει μόνο μια διεύθυνση IP, δεν υπάρχει τρόπος να καθοριστεί ποιον εσωτερικό πελάτη θέλει κάθε φορά να προσεγγίσει. Αυτό απαγορεύει σε εισβολείς να συνδεθούν σε εσωτερικούς πελάτες, αλλά επίσης απαγορεύει τη σύνδεση και των νόμιμων χρηστών. Ευτυχώς, οι περισσότερες σύγχρονες υλοποιήσεις NAT επιτρέπουν την δημιουργία κανόνων προώθησης θύρας, οι οποίοι επιτρέπουν την προσέγγιση εσωτερικών ξενιστών.

Τα Windows 2000 και XP, το Unix και πολλά σύγχρονα λειτουργικά συστήματα παρέχουν αυτήν τη λειτουργία ως τμήμα της διανομής του λειτουργικού συστήματος. Τα Windows NT δεν την παρέχουν.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Κατά τη μελέτη και συγγραφή της παρούσας πτυχιακής αρχικά μάθαμε πολλά πράγματα σχετικά με την ασφάλεια τόσο στο διαδίκτυο όσο και στην αποστολή/λήψη των emails.

Έχει καταστεί σαφές ποιοι είναι οι κίνδυνοι του διαδικτύου και με ποιους τρόπους μπορούν να αντιμετωπιστούν, ώστε να παρέχεται μια ασφαλής περιήγηση στο internet. Παράλληλα, μελετήθηκαν βιβλιογραφικά οι διάφορες πιθανές επιθέσεις μέσω του email (phishing, pharming, spoofing), τι σημαίνει και πού αποσκοπεί η κάθε μια, ενώ δόθηκαν οι βέλτιστοι τρόποι αντιμετώπισης αυτών των επιθέσεων, τόσο από την πλευρά μιας εταιρίας που θέλει να διατηρήσει την καλή φήμη της, όσο και από την πλευρά των χρηστών/πελατών, ώστε να μην κινδυνεύουν τα προσωπικά τους δεδομένα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] “A classical introduction to cryptography, Applications for communication security”, Serge Vaudenay, Springer, 2006

[2] “Computer Network Security”, Joseph Migga Kizza, Springer, 2005

[3] “Network intrusion detection and prevention – Concepts and Techniques”, Ali A. Ghorbani, Wei Lu and Mahbod Tavallaee, Springer, 2010

[4] “Network security policies and procedues”, Douglas W. Frye, Springer, 2007

[5] “Ασφάλεια Δικτύων Υπολογιστών – Τεχνολογίες και υπηρεσίες σε περιβάλλοντα ηλεκτρονικού επιχειρείν και ηλεκτρονικής διακυβέρνησης”, Στέφανος Γκριτζάλης και Σωκράτης Κάτσικας, Εκδόσεις Παπασωτηρίου

[6] www.wikipedia.com

[7] http://www.darkreading.com/document.asp?doc_id=110384

[8] http://palisade.plynt.com/issues/2006Mar/pharming/