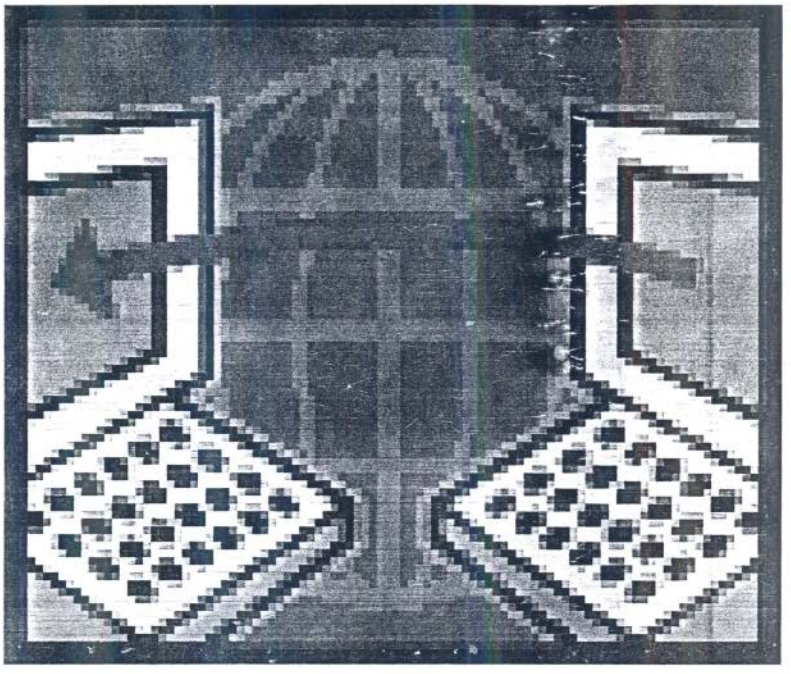
188

ΔΙΑΣΦΑΛΙΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ ΣΤΟ INTERNET



Πετρίκης Ανδρέας
Τούφας Κωνσταντίνος

Πτυχιακή εργασία
Υπεύθυνος καθηγητής:Τσιαντής Λεωνίδας

Τμήμα Τηλεπληροφορικής και διοίκησης

Τεχνολογικό Εκπαιδευτικό Ίδρυμα (Τ.Ε.Ι) Ηπείρου

ΠΕΡΙΕΧΟΜΕΝΑ

Μάλιστα όπως τονίζει η Jupiter , πολλές εταιρείες με κακές πρακτικές σε αυτόν τον τομέα μπορεί να δουν τα έσοδα τους να μειώνονται όχι μόνο στις online πωλήσεις αλλά και στις offline.

1.Εισαγωγή

Οι ανησυχίες για την ασφάλεια των ηλεκτρονικών δικτύων και των συστημάτων πληροφόρησης έχουν αυξηθεί μαζί με την γρήγορη αύξηση στον αριθμό χρηστών του δικτύου και την αξία των συναλλαγών τους. Η ασφάλεια έχει φθάσει τώρα σε ένα κρίσιμο σημείο όπου αντιπροσωπεύει μία αναγκαία προϋπόθεση για την αύξηση των ηλεκτρονικών επιχειρήσεων και την λειτουργία ολόκληρης της οικονομίας. Διάφοροι παράγοντες έχουν συνδυάσει να ωθήσουν την ασφάλεια ενημέρωσης και επικοινωνίας στην κορυφή της πολιτικής ημερήσιας διάταξης στην Ε.Ε:

Οι κυβερνήσεις έχουν συνειδητοποιήσει τον βαθμό στον οποίον τα οικονομικά τους και οι πολίτες τους εξαρτώνται από την αποτελεσματική εργασία των δικτύων επικοινωνίας και αρκετές έχουν αρχίσει να αναθεωρούν τις ρυθμίσεις ασφαλείας τους.
Το διαδίκτυο έχει δημιουργήσει μία σύνδεση σφαιρικής συνδεκτικότητας εκατομμυρίων μαζί δικτύων, μεγάλα και μικρά, και εκατοντάδες εκατομμύρια μεμονωμένους υπολογιστές, και όλο και περισσότερες άλλες συσκευές συμπεριλαμβανομένων κινητών τηλεφώνων. Αυτό έχει μειώσει σημαντικά τις δαπάνες στις πολύτιμες πληροφορίες για τους μακρινούς επιτιθέμενους.
Έχουν υπάρξει μερικοί ιοί που απελευθερώνονται στο διαδίκτυο που προκαλούν την εκτενή ζημία με την καταστροφή των πληροφοριών και την άρνηση πρόσβασης στο δίκτυο. Τέτοια προβλήματα ασφάλειας δεν είναι περιορισμένα στις μεμονωμένες χώρες αλλά εξαπλώνονται γρήγορα σε κράτη μέλη.

Ενώ η ασφάλεια έχει γίνει η βασική πρόκληση για τους φορείς χάραξης πολιτικής, η εύρεση μιας επαρκούς πολιτικής απάντησης γίνεται ένα όλο και περισσότερο σύνθετο θέμα. Μόνο μερικά έτη πριν η ασφάλεια δικτύων ήταν κυρίως ένα ζήτημα για τα κρατικά μονοπώλια που προσφέρουν τις ειδικευμένες υπηρεσίες που έδρευαν στα δημόσια δίκτυα, ειδικότερα το τηλεφωνικό δίκτυο. Η ασφάλεια των συγκροτημάτων ηλεκτρονικών υπολογιστών περιοριζότανε στις μεγάλες οργανώσεις και εστιαζότανε στους ελέγχους πρόσβασης. Η πολιτική ασφάλειας ήταν έργο μίας σχετικά απλής κατάστασης. Αυτή η κατάσταση έχει τώρα αλλάξει αρκετά λόγω ποικίλων εξελίξεων στο ευρύτερο πλαίσιο αγοράς, μεταξύ αυτών της φιλελευθεροποίησης, της σύγκλισης και παγκοσμιοποίησης.
Τα δίκτυα τώρα κυρίως είναι ιδιωτικοποιημένα και αυτοδιαχειριζόμενα Οι πληροφορίες προσφέρονται σε ανταγωνιστική

βάση με την ασφάλεια ως τμήμα της αγοράς προσφοράς. Ωστόσο πολλοί πελάτες παραμένουν αμαθείς στην επέκταση των κινδύνων ασφαλείας που διατρέχουν κατά την σύνδεση με ένα δίκτυο και συνεπώς λαμβάνουν τις αποφάσεις τους σε μία κατάσταση ελλιπούς πληροφόρησης.
Τα δίκτυα και τα συστήματα πληροφοριών συγκλίνουν. Γίνονται όλο και περισσότερο διασυνδεόμενα, προσφέροντας το ίδιο είδος άνευ ραφής και εξατομικευμένων υπηρεσιών και σε μερικά επεκτείνουν την διανομή με την ίδια υποδομή. Τερματικά όπως υπολογιστές και κινητά τηλέφωνα έχουν γίνει ένα ενεργό στοιχείο στη δικτυακή αρχιτεκτονική και μπορούν να συνδεθούν σε διαφορετικά δίκτυα.
Τα δίκτυα είναι διεθνή. Ένα σημαντικό μέρος της σημερινής επικοινωνίας είναι διασυνοριακό ή διέρχεται μέσω τρίτων χωρών(μερικές φορές χωρίς τον τελικό χρήστη που το γνωρίζει), έτσι οποιαδήποτε λύση σε έναν κίνδυνο ασφαλείας πρέπει να λάβει υπόψη αυτό. Τα περισσότερα δίκτυα χτίζονται χρησιμοποιώντας εμπορικά προϊόντα από διεθνείς πωλητές. Τα προϊόντα ασφαλείας πρέπει να είναι συμβατά με τα διεθνή πρότυπα.

2.Ασφάλεια δικτύων και πληροφοριών

2.1 Καθορισμός της ασφάλειας

Τα δίκτυα είναι συστήματα στα οποία αποθηκεύονται πληροφορίες, επεξεργάζονται και διαμέσου αυτών κυκλοφορούν. Είναι συγκροτημένα μέσω συστατικών μετάδοσης (καλώδια, ασύρματες ενώσεις, δορυφόρους, πύλες, διακόπτες κτλ) και υποστηρίζουν υπηρεσίες. Προσκολλημένη στα δίκτυα είναι μια αυξανόμενη πλατιά έκταση από εφαρμογές (συστήματα μεταφοράς email, κατανεμητές κτλ) και εξοπλισμός τερματικών (τηλέφωνα, προσωπικοί υπολογιστές, κινητά τηλέφωνα, προσωπικές αντζέντες, οικιακές συσκευές, βιομηχανικές μηχανές, κτλ). Οι προϋποθέσεις μιας γενικής ασφάλειας των δικτύων και των συστημάτων πληροφοριών πρέπει να αποτελείται από τα παρακάτω αλληλοσυσχετισμένα χαρακτηριστικά:
i) **Διαθεσιμότητα**- σημαίνει ότι οι πληροφορίες είναι προσβάσιμες και οι υπηρεσίες είναι λειτουργικές, παρά πιθανά αποσυνδετικά γεγονότα όπως η διακοπή παροχής ενέργειας, φυσικές καταστροφές, ατυχήματα ή επιθέσεις. Αυτό είναι ειδικά ζωτικό σε περιβάλλοντα όπου αποτυχίες στην επικοινωνία των δικτύων μπορεί να προκαλέσουν κατάρρευση σε άλλα κρίσιμα δίκτυα όπως οι αεροπορικές μεταφορές ή η παροχή ρεύματος.
ii) **Πιστοποίηση**- είναι η επιβεβαίωση ταυτότητας ονομάτων ή χρηστών. Κατάλληλες μέθοδοι πιστοποίησης χρειάζονται για πολλές εφαρμογές και υπηρεσίες όπως περιλαμβάνοντας μια τηλεφωνική σύναψη,

ελέγχοντας πρόσβαση σε συγκεκριμένες πληροφορίες και υπηρεσίες και πιστοποίηση ιστιοσελίδων. Η πιστοποίηση πρέπει επίσης να περιλαμβάνει την πιθανότητα για ανωνυμία, αφού πολλές υπηρεσίες δεν χρειάζονται την ταυτότητα του χρήστη, αλλά μόνο μία αξιόπιστη επιβεβαίωση συγκεκριμένων κριτηρίων, όπως την ικανότητα πληρωμής.
iii) **Ακεραιότητα-** είναι η επιβεβαίωση ότι η πληροφορία που έχει σταλθεί, έχει φτάσει, ή έχει αποθηκευτεί είναι ολοκληρωμένη και άθικτη. Αυτό είναι απαραίτητο σε σχέση με την πιστοποίηση για την ολοκλήρωση συμβολαίων ή όπου η ακρίβεια της πληροφορίας είναι κρίσιμη.
iv) **Εμπιστευτικότητα-** είναι η προστασία των επικοινωνιών ή των αποθηκευμένων πληροφοριών εναντίον ανάσχεσης και ατόμων χωρίς αρχή. Συγκεκριμένα χρειάζεται για την μεταφορά ευαίσθητων πληροφοριών και είναι μια από τις απαιτήσεις στις ιδιωτικές διευθύνσεις όσον αφορά τους χρήστες των δικτύων τηλεπικοινωνίας. Όλα τα γεγονότα που απειλούν την ασφάλεια πρέπει να καλυφθούν, όχι μόνο αυτά με μοχθηρούς σκοπούς. Από την πλευρά του χρήστη, κίνδυνοι όπως ατυχήματα περιβάλλοντος ή ανθρώπινα λάθη τα οποία διαλύουν το δίκτυο κοστίζουν ενδεχομένως όσο οι μοχθηρές επιθέσεις.

2.2 Τύποι επιθέσεων εναντίον πληροφοριακών συστημάτων

Η φράση πληροφοριακό σύστημα χρησιμοποιείται σκόπιμα σε μια δικιά της ευρεία αίσθηση όσον αφορά την σύγκλιση μεταξύ των δικτύων ηλεκτρονικής επικοινωνίας και διάφορων συστημάτων τα οποία επικοινωνούν. Για τον σκοπό αυτής της πρότασης, τα συστήματα πληροφοριών περιλαμβάνουν προσωπικούς υπολογιστές, προσωπικούς ψηφιακούς organisers, κινητά τηλέφωνα, εσωτερικά δίκτυα, εξωτερικά και φυσικά, δίκτυα, υπολογιστές εξυπηρέτησης δικτύου και άλλες υποδομές του INTERNET.
Οι απειλές εναντίον υπολογιστικών συστημάτων είναι οι εξής:
(α) Μη ελεγχόμενη πρόσβαση σε πληροφοριακά συστήματα. Αυτό περιλαμβάνει την έννοια του hacking.Το hacking πραγματοποιείται με την πρόσβαση κάποιου χωρίς να έχει το δικαίωμα σε έναν υπολογιστή ή σε ένα δίκτυο υπολογιστών. Μπορεί να συμβεί με μια ποικιλία τρόπων απλά προωθώντας μέσα στην πληροφορία μέσω επιθέσεων και κλέψιμο κωδικών. Συχνά-όχι όμως πάντα- αντιγράφοντας, αλλάζοντας ή καταστρέφοντας πληροφορίες. Σκόπιμη διακοπή ιστοσελίδων ή πρόσβασης σε υπηρεσίες που προστατεύονται από υποθετικές προσβάσεις χωρίς πληρωμή μπορεί να είναι ένας από τους στόχους του hacking.

(β) Διάσπαση των πληροφοριακών συστημάτων. Διαφορετικοί τρόποι υπάρχουν για να διασπούν τα πληροφοριακά συστήματα μέσω μοχθηρών επιθέσεων. Ένας από τους καλύτερα γνωστούς τρόπους να αρνηθείς ή να αλλοιώσεις τις υπηρεσίες που προσφέρονται από το διαδίκτυο είναι μια ΄΄άρνηση υπηρεσίας΄΄ επίθεσης. Αυτή η επίθεση είναι παρόμοια των μηχανών του fax οι οποίες είναι όμηροι από μεγάλα και επαναλαμβανόμενα μηνύματα. Η άρνηση τέτοιων υπηρεσιών προσπαθεί να υπερφορτώσει τους servers ή τους providers με αυτοματοποιημένα μηνύματα. Άλλοι τύποι επιθέσεων μπορούν να περιλαμβάνουν διασπασμένους servers λειτουργώντας το domain name system(DNS) και επιθέσεις κατευθυνόμενες στους κατανεμητές. Οι επιθέσεις που σκοπεύουν στην διάσπαση των συστημάτων ήταν καταστροφικές για συγκεκριμένες υψηλού προφίλ ιστοσελίδες όπως οι πύλες. Κάποιοι αναφορές υπολόγισαν ότι μια πρόσφατη επίθεση κόστισε ζημιά ύψους εκατοντάδων χιλιάδων ευρώ, όπως επίσης απροσδιόριστη ζημιά στην φήμη. Όλο και περισσότερο, εταιρίες εφησυχάζουν στην διαθεσιμότητα των ιστοσελίδων τους για τις εργασίες τους και αυτές που στηρίζονται σε αυτό είναι ιδιαιτέρως ευαίσθητες.

(γ) Εκτέλεση του κακού λογισμικού που αλλάζει ή καταστρέφει τις πληροφορίες. Ο πιο γνωστός τύπος κακού λογισμικού είναι ο ιός. Κακόφημα παραδείγματα ιών: "I Love you", "Melissa", "Kournikova". Περίπου 11% των ευρωπαίων χρηστών έχει δεχτεί ιό στον προσωπικό υπολογιστή τους. Υπάρχουν και άλλοι τύποι κακού λογισμικού. Κάποιοι χρησιμοποιούν τον υπολογιστή για να επιτεθούν σε άλλους. Κάποια προγράμματα (που συχνά ονομάζονται 'logic bombs') μπορούν να μένουν κρυφά μέχρι να ενεργοποιηθούν από κάποιο γεγονός όπως μια συγκεκριμένη ημερομηνία, στο σημείο που μπορούν να προκαλέσουν μεγάλη ζημιά αλλάζοντας ή διαγράφοντας πληροφορίες. Άλλα προγράμματα φαίνονται κανονικά, αλλά όταν ανοίγουν ελευθερώνουν μια επίθεση (συχνά λέγεται 'Trojan Horses'). Άλλη μια παραλλαγή είναι ένα πρόγραμμα (συχνά ονομάζεται σκουλήκι) το οποίο δεν μολύνει άλλα προγράμματα όπως ο ιός, αλλά αντί για αυτό δημιουργεί αντίγραφα του εαυτού του, το οποίο διαδοχικά δημιουργεί ακόμη περισσότερα αντίγραφα και που τελικά βυθίζει το σύστημα.

(δ) Ανάσχεση των επικοινωνιών. Οι διακοπές των επικοινωνιών εκθέτουν τις εμπιστευτικές και ευσταθείς απαιτήσεις των χρηστών. Αυτό συχνά ονομάζεται 'sniffing'.

(ε) Ψεύτικη καταχώρηση στοιχείων. Τα συστήματα πληροφοριών προσφέρουν νέες ευκαιρίες για ψεύτικες καταχωρήσεις στοιχείων. Το να παίρνεις κάποιου άλλου την ταυτότητα στο διαδίκτυο, και να την χρησιμοποιείς για κακούς σκοπούς, αυτό συχνά ονομάζεται "spoofing".

2.3 Η φύση της απειλής

Μερικά από τα πιο σοβαρά ατυχήματα των επιθέσεων εναντίον συστημάτων πληροφοριών κατευθύνονται εναντίον διαχειριστών δικτύων ηλεκτρονικών επικοινωνιών και προμηθευτών υπηρεσιών ή εναντίον εταιριών ηλεκτρονικών συναλλαγών. Τα θύματα των επιθέσεων δεν είναι μόνο οργανισμοί, μπορεί να υπάρξουν πολύ άμεσα, σοβαρά και καταστροφικά αποτελέσματα σε ιδιώτες επίσης. Η οικονομική επιβάρυνση επιβάλλεται από συγκεκριμένες από αυτές τις επιθέσεις σε δημόσια πρόσωπα, εταιρίες και ιδιώτες και γίνονται τα συστήματα πληροφοριών πιο δαπανηρά και λιγότερο ανεκτά στους χρήστες.

Οι τύποι των επιθέσεων που περιγράφονται παρακάτω συχνά εκτελούνται από ιδιώτες που ενεργούν από μόνοι τους, μερικές φορές από διάφορους που δεν έχουν συνολική εκτίμηση της σοβαρότητας των πράξεων τους. Ωστόσο το επίπεδο του σχεδιασμού και της φιλοδοξίας της επιθέσεως μπορεί να μεγαλώσει. Υπάρχει μεγάλο και ανήσυχο ενδιαφέρον των οργανωμένων εγκληματιών που χρησιμοποιούν δίκτυα επικοινωνιών για να ξεκινήσουν επιθέσεις εναντίον συστημάτων πληροφοριών για δικούς τους σκοπούς. Οργανωμένες ομάδες hacking που ειδικεύονται στο hacking και στην παραμόρφωση των ιστοσελίδων είναι όλο και πιο ενεργές στο παγκόσμιο επίπεδο. Η σύλληψη μεγάλων ομάδων από hackers δείχνει ότι το hacking μπορεί αυξανόμενα να γίνει φαινόμενο οργανωμένου εγκλήματος. Υπήρξαν πρόσφατα μεθοδευμένες και οργανωμένες επιθέσεις εναντίον πνευματικής περιουσίας όπως επίσης προσπάθειες να κλαπούν μεγάλα ποσά από τραπεζικές υπηρεσίες.

Κανόνες παραβίασης ασφάλειας σε βάσεις δεδομένων ηλεκτρονικής εμπορικής συναλλαγής, που περιλαμβάνουν αριθμούς πιστωτικών καρτών, είναι επίσης ένας λόγος για ανησυχία. Αυτές οι επιθέσεις είναι αποτέλεσμα αυξανόμενων ευκαιριών για οικονομικό έγκλημα και σε κάθε περίπτωση αναγκάζουν την τραπεζική βιομηχανία να διακόψει και να επανεξετάσει χιλιάδες καρτών. Μια μακρύτερη σκέψη είναι η απροσδιόριστη ζημιά στην φήμη των εμπόρων και στην καταναλωτική εμπιστοσύνη του ηλεκτρονικού εμπορίου. Προληπτικά μέτρα, όπως οι ελάχιστες απαιτήσεις ασφάλειας για απευθείας συναλλαγές δέχοντας πιστωτικές κάρτες, συζητιούνται στο σχέδιο δράσης για να αποτρέψουν το οικονομικό έγκλημα.

3.Η ανάγκη για μια πολιτική

Η προστασία των δικτύων επικοινωνίας αυξάνεται σεβαστά όσο η προτεραιότητα για δημιουργία πολιτικής κυρίως εξαιτίας της προστασίας πληροφοριών, εξασφαλίζοντας μια λειτουργική οικονομία, εθνική ασφάλεια, και την ευχή να προοδεύσει το ηλεκτρονικό εμπόριο. Αυτό οδήγησε σε ένα σώμα περιεχομένων από νόμιμες ασφάλειες στις διαταγές της ΕΕ πάνω στην ασφάλεια των πληροφοριών και στο ρυθμιστικό πλαίσιο της ΕΕ για τις τηλεπικοινωνίες. Ωστόσο αυτά τα μέτρα πρέπει να εφαρμοστούν σε ένα γρήγορα αλλαγμένο περιβάλλον νέων τεχνολογιών, ανταγωνιστικών αγορών, σύγκλισης των δικτύων, και παγκοσμιοποίησης. Αυτές οι προκλήσεις αυξάνονται με το γεγονός ότι η αγορά θα προσπαθήσει να υποκαθιστήσει την ασφάλεια για λόγους που αναλύονται παρακάτω.

Η ασφάλεια των πληροφοριών και των δικτύων είναι ένα εμπόρευμα που αγοράστηκε και πουλήθηκε στην αγορά και μέρος των συμβατικών συμφωνιών μεταξύ των χωρών. Η αγορά για τα προϊόντα ασφαλείας έχει αυξηθεί σημαντικά τα τελευταία χρόνια. Σύμφωνα με κάποιες αναφορές η αγορά για το λογισμικό της ασφάλειας του διαδίκτυου έφτασε γύρω στα 4.4 εκατομμύρια δολάρια παγκοσμίως στο τέλος του 1999 και θα αυξηθεί 23% για να φτάσει το 2004 τα 8.3 εκατομμύρια δολάρια. Στην Ευρώπη, η αγορά ασφάλειας ηλεκτρονικών επικοινωνιών προβλέπεται να αυξηθεί από 465 χιλιάδες δολάρια το 2000 σε 5.3 εκατομμύρια το 2006, με την αγορά ασφάλειας για τεχνολογίες πληροφοριών να αυξάνεται από 490 χιλιάδες δολάρια το 1999 σε 2.74 εκατομμύρια το 2006.

Η εμπλεκόμενη ανάληψη που συνήθως γίνεται είναι ότι η μηχανική τιμή θα ισορροπήσει τα κόστη εξασφαλίζοντας την ασφάλεια με την συγκεκριμένη ανάγκη για ασφάλεια. Κάποιοι χρήστες θα απαιτήσουν υψηλή ασφάλεια ενώ άλλοι θα είναι ικανοποιημένοι με ένα χαμηλότερο επίπεδο εγγύησης. Οι προτιμήσεις τους θα έχουν επηρεαστεί στην τιμή που θέλουν να πληρώσουν μέτρα ασφαλείας. Ωστόσο, πολλά ρίσκα ασφαλείας παραμένουν άλυτα ή οι λύσεις έρχονται αργά στην αγορά σαν αποτέλεσμα συγκεκριμένων ατελειών της αγοράς:
i) Κοινωνικά κόστη και οφέλη: Η επένδυση στην βελτιωμένη ασφάλεια δικτύων γεννά κοινωνικά κόστη και οφέλη, τα οποία δεν είναι επαρκώς απεικονισμένα στην αγορά τιμών. Στην μεριά του κόστους, οι θιασώτες της αγοράς δεν είναι υπεύθυνοι για όλα τα χρέη σχετικά με την συμπεριφορά τους ως προς την ασφάλεια. Οι χρήστες και οι κατανεμητές με χαμηλά επίπεδα ασφαλείας δεν χρειάζεται να πληρώσουν τρίτου μέρους ευθύνη. Παρόμοια, στο διαδίκτυο μερικές επιθέσεις που έχουν φθάσει μέχρι τις ασύνετες μηχανές των σχετικά απρόσεχτων χρηστών. Τα κέρδη της ασφάλειας δεν είναι ωστόσο εντελώς επηρεασμένα στις τιμές αγοράς. Όταν διαχειριστές, προμηθευτές, ή κατανεμητές υπηρεσιών

δικτύων και πληροφοριών μπορεί να περιγραφεί παρακάτω. Πρώτον, τα νόμιμα άρθρα στο επίπεδο της Ε.Ε πρέπει να εφαρμοστούν αποτελεσματικά, που αυτό απαιτεί μια κοινή κατανόηση των βασικών θεμάτων ασφάλειας και των συγκεκριμένων μέτρων που πρέπει να παρθούν. Το νόμιμο πλαίσιο θα χρειαστεί επίσης να αναπτυχθεί στο μέλλον αφού ήδη φαίνεται από το προτεινόμενο νέο ρυθμιστικό πλαίσιο για ηλεκτρονικές επικοινωνίες ή από τις νέες προτάσεις στην συζήτηση για το ηλεκτρονικό έγκλημα. Δεύτερον, συγκεκριμένες ατέλειες της αγοράς οδηγούν στο συμπέρασμα ότι οι δυνάμεις της αγοράς δεν κάνουν μεγάλες επενδύσεις στην τεχνολογία ή στην εφαρμογή της ασφάλειας. Τα πολιτικά μέτρα μπορούν να ενισχύσουν την διαδικασία της αγοράς και την ίδια ώρα να βελτιώσουν την λειτουργία του νόμιμου πλαισίου. Τέλος, οι υπηρεσίες επικοινωνιών και πληροφοριών προσφέρονται παγκοσμίως. Συνεπώς, μια διαδικασία Ευρωπαϊκής πολιτικής χρειάζεται για να διασφαλίσει την εσωτερική αγορά, για να πλεονεκτεί από κοινές λύσεις, και για να είναι ικανή να ενεργήσει σε παγκόσμιο επίπεδο.

4. Προτεινόμενα μέτρα

Είναι γεγονός ότι τα τελευταία χρόνια η Ευρωπαϊκή νομοθεσία έχει αναπτυχθεί μέσω σημαντικών αποφάσεων για την καταπολέμηση του ηλεκτρονικού εγκλήματος. Όπως με τα νομοθετικά μέτρα, πρέπει επίσης να παρθούν και άλλα μέτρα. Αυτά περιλαμβάνουν τα ακόλουθα:

1) **Ανάταση της επίγνωσης:** Μια δημόσια καμπάνια ενημέρωσης και εκπαίδευσης πρέπει να εφαρμοστεί και καλύτερες πρακτικές πρέπει να προωθηθούν.
2) **Ένα ευρωπαϊκό σύστημα προειδοποίησης και πληροφοριών:** Τα κράτη μέλη πρέπει να δυναμώσουν τις ομάδες υπολογιστών ανταπόκρισης ανάγκης και να βελτιώσουν την συνεργασία μεταξύ αυτών.
3) **Τεχνολογική υποστήριξη:** Η υποστήριξη για έρευνα και ανάπτυξη στην ασφάλεια πρέπει να είναι ένα γεγονός κλειδί για τα προγραμματικά πλαίσια και να ενώνεται με την ευρύτερη στρατηγική για βελτιωμένη ασφάλεια δικτύων και πληροφοριών.
4) **Υποστήριξη για αγορά προσανατολισμένη στην προτυποποίηση και στην πιστοποίηση:** Οι ευρωπαϊκοί οργανισμοί προτυποποίησης έγιναν για να γίνεται σταδιακά γρηγορότερα η εργασίες στον τομέα της ασφάλειας.
5) **Ασφάλεια στην λειτουργία της κυβέρνησης:** Τα κράτη μέλη πρέπει να ενσωματώνουν αποτελεσματικά τις ενδοτμηματικές λύσεις ασφάλειας στις δικές τους ηλεκτροκυβερνητικές

δραστηριότητες. Τα κράτη μέλη πρέπει να παρουσιάζουν ηλεκτρονικές υπογραφές όταν προσφέρουν δημόσιες υπηρεσίες.

6) **Διεθνής συνεργασία:** Η Ε.Ε θα επαναφέρει τον διάλογο με διεθνείς οργανισμούς και συνεργάτες στην ασφάλεια δικτύων και πληροφοριών.

5.1 Computer-related crime

Υπάρχουν πολλές απόψεις στο τι αποτελεί 'computer-related crime'. Οι όροι 'computer crime', 'computer-related crime', 'cybercrime' συχνά χρησιμοποιούνται εναλλακτικά. Μια διαφορά μπορεί να υπάρξει μεταξύ συγκεκριμένων υπολογιστικών εγκλημάτων και παραδοσιακών εγκλημάτων που εκτελούνται με την βοήθεια της τεχνολογίας των υπολογιστών. Αν και τα συγκεκριμένα εγκλήματα 'υπολογιστών' απαιτούν ενημερώσεις των ορισμών των εγκλημάτων στους κώδικες εθνικού εγκλήματος, τα παραδοσιακά εγκλήματα εκτελούνται με την βοήθεια υπολογιστών που καλούνται για την βελτίωση των μέτρων της συνεργασίας και της διαδικασίας.

Σαν μέρος του σχεδίου δράσης Ευρώπη του 2000 η Ευρωπαϊκή Ένωση εξέδωσε μια ανακοίνωση έχοντας τον τίτλο "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime". Αυτή η ανακοίνωση πρότεινε μια ισορροπημένη προσέγγιση των προβλημάτων του ηλεκτρονικού εγκλήματος, παίρνοντας πλήρης εκτίμηση των απόψεων όλων των ενδιαφερόμενων περιλαμβάνοντας πρακτορεία εφαρμογής νόμων, προμηθευτές υπηρεσιών, διαχειριστές δικτύων, διάφορες βιομηχανικές εταιρίες, καταναλωτικές ομάδες, αρχές προστασίας δεδομένων και ιδιωτικές ομάδες. Η ανακοίνωση πρότεινε έναν αριθμό νομοθετικών και μη νομοθετικών πρωτοβουλιών. Ένας από τους πιο απαραίτητους και αποτελεσματικούς τρόπους για να διεκπεραιωθούν αυτά τα προβλήματα είναι μέσω της πρόληψης και της εκπαίδευσης. Η ανακοίνωση υπογράμμισε την σημαντικότητα της διαθεσιμότητας, της εξέλιξης, της ανάπτυξης και της αποτελεσματικής χρήσης των προληπτικών τεχνολογιών. Τονίστηκε ότι υπάρχει μια ανάγκη να αφυπνιστεί η συνείδηση του κοινού πάνω στους κινδύνους που προκαλεί το ηλεκτρονικό έγκλημα, να προωθηθούν οι καλύτερες πρακτικές για την ασφάλεια, να αναπτυχθούν αποτελεσματικά εργαλεία και πρωτόκολλα για να καταπολεμηθεί το ηλεκτρονικό έγκλημα ως επίσης και η ενθάρρυνση μεγαλύτερης ανάπτυξης προειδοποιητικών μηχανισμών και μηχανισμών διαχείρισης κρίσεων. Το πρόγραμμα της Information Society Technologies (IST) παρέχει ένα πλαίσιο για την ανάπτυξη δυνατοτήτων και τεχνολογιών για την κατανόηση επειγουσών προκλήσεων που σχετίζονται με το ηλεκτρονικό έγκλημα.

Το 2001 ολοκληρώθηκε το συμβούλιο της Ευρωπαϊκής σύμβασης για το ηλεκτρονικό έγκλημα. Καταλήγει στο ότι:

• εναρμονίζονται νόμοι που αναλαμβάνουν τα αδικήματα του ηλεκτρονικού εγκλήματος
• προωθούνται διαδικαστικές εξουσίες που είναι απαραίτητες για την έρευνα και την δίωξη αυτών των αδικημάτων και
• δημιουργείται ένα σύστημα παγκόσμιας συνεργασίας.

Τα αδικήματα που περιλαμβάνονται στην σύμβαση είναι:

• αδικήματα εναντίον της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των συστημάτων και των δεδομένων των υπολογιστών. Αυτά περιλαμβάνουν παράνομη πρόσβαση, παράνομη ανάσχεση, παρεμβολή δεδομένων, παρεμβολή συστημάτων και κακομεταχείριση συσκευών.
• αδικήματα ηλεκτρονικού εγκλήματος. Αυτά περιλαμβάνουν παραποίηση και απάτη μέσω υπολογιστών
• αδικήματα σχετικά με την ικανοποίηση των επιθυμιών κάποιου. Αυτά είναι αδικήματα που σχετίζονται με την παιδική πορνογραφία.
• αδικήματα που σχετίζονται με τις καταπατήσεις των δικαιωμάτων των δημιουργών. Αυτά είναι αδικήματα που σχετίζονται με την παράνομη αντιγραφή και αναπαραγωγή ψηφιακών δίσκων κ.τ.λ

Επιπλέον το 2003 η Ευρωπαϊκή Ένωση ανακοίνωσε την δημιουργία ενός πρακτορείου ηλεκτρονικού εγκλήματος με σκοπό να συντονίζει τα εφόδια συνεργασίας μεταξύ των χωρών μελών, αλλά επίσης και με άλλες χώρες, για την βελτίωση της ασφάλειας και της καταπολέμησης του ηλεκτρονικού εγκλήματος.

5.2 Πλαίσιο στις επιθέσεις εναντίον υπολογιστικών συστημάτων

Στις 23-24 Μαρτίου στην Στοκχόλμη το Ευρωπαϊκό Συμβούλιο αναγνώρισε την ανάγκη για περαιτέρω δράση στον χώρο της ασφάλειας των δικτύων και των πληροφοριών και κατέληξε " το Συμβούλιο μαζί με την Ευρωπαϊκή Ένωση θα αναπτύξουν μια πολυσήμαντη στρατηγική στην ασφάλεια των ηλεκτρονικών δικτύων περιλαμβάνοντας πρακτικής εφαρμογής δράση." Η Ένωση ανταποκρίθηκε στο κάλεσμα αυτό με μια ανακοίνωση της στην "ασφάλεια δικτύων και πληροφοριών: μια προσέγγιση Ευρωπαϊκής Πολιτικής". Αυτό ανάλυε τα επίκαιρα προβλήματα στην ασφάλεια δικτύων, και προέβλεπε μια στρατηγική σε γενικές γραμμές για δράση στην περιοχή αυτή. Ακολούθησε ένα συμβούλιο αποφάσεων στις 6 Δεκεμβρίου του 2001 σε μια κοινή προσέγγιση και συγκεκριμένες ενέργειες στον τομέα ασφάλειας δικτύων και πληροφοριών.

Αυτές οι πρωτοβουλίες από μόνες τους δεν είναι επαρκείς για να διασφαλίσουν όλες τις απαραίτητες αντιδράσεις σε σοβαρές επιθέσεις εναντίον συστημάτων πληροφοριών. Και οι δύο ανακοινώσεις αναγνώρισαν ότι υπάρχει μια επείγουσα ανάγκη για προσέγγιση του νόμου περί διαρκούς εγκλήματος εντός της Ευρωπαϊκής Ένωσης στον τομέα των επιθέσεων εναντίον συστημάτων πληροφοριών. Το 2002 η Ένωση έθεσε μια πρόταση για ένα συμβούλιο πλαισίου στις ' επιθέσεις εναντίον συστημάτων πληροφοριών', το οποίο είχε ως σκοπό να προσεγγίσει το νόμο περί εγκλήματος διά μέσου της Ευρωπαϊκής Ένωσης, για να διασφαλίσει ότι η εφαρμογή του Ευρωπαϊκού νόμου και οι δικαστικές αρχές μπορούν να πάρουν πρωτοβουλία εναντίον αυτού του νέου είδους εγκλήματος. Επίσης είχε σκοπό να παροτρύνει και να προωθήσει την ασφάλεια πληροφοριών. Το πλαίσιο της απόφασης, το οποίο τώρα έχει προταθεί, προσφωνεί τον πυρήνα του ηλεκτρονικού εγκλήματος προτείνοντας ένα νομικό έγγραφο που θα προσέγγιζε τους νομικούς κανόνες του εγκλήματος κα θα διευκόλυνε την δικαστική συνεργασία για:

- παράνομη πρόσβαση σε συστήματα πληροφοριών ("hacking")
- παράνομη παρέμβαση σε συστήματα πληροφοριών (η διακίνηση επικίνδυνων κωδικών, κοινώς γνωστούς ως ιούς).

Οι νόμοι των κρατών-μέλη σε αυτόν τον τομέα περιλαμβάνουν κάποια σημαντικά χάσματα και διαφορές που θα μπορούσαν να επέμβουν εμποδίζοντας τον αγώνα ενάντια στο οργανωμένο έγκλημα και στην τρομοκρατία, όπως επίσης σοβαρές επιθέσεις από μεμονωμένα άτομα εναντίον συστημάτων πληροφοριών. Η προσέγγιση σημαντικών νόμων στον χώρο του εγκλήματος υψηλής τεχνολογίας θα διασφαλίσει ότι η διεθνής νομοθεσία έχει αρκετά μεγάλο εύρος έτσι ώστε όλοι οι τύποι των σοβαρών επιθέσεων εναντίον συστημάτων πληροφοριών να μπορούν να διερευνούνται χρησιμοποιώντας τεχνικές και μεθόδους διαθέσιμες στον νόμο του εγκλήματος. Οι δράστες αυτών των αδικημάτων πρέπει να αναγνωρίζονται, να έρχονται ενώπιον της δικαιοσύνης, και τα δικαστήρια πρέπει να έχουν κατάλληλες και ανάλογες ποινές στην διάθεση τους. Αυτό θα στείλει ένα δυνατό και αποθαρρυντικό μήνυμα σε αυτούς που μελετούν επιθέσεις εναντίον συστημάτων πληροφοριών.

Άλλωστε, αυτά τα χάσματα και οι διαφορές μπορεί να ενεργήσουν σαν ένα εμπόδιο στην αποτελεσματική αστυνόμευση και δικαστική συνεργασία στον τομέα των επιθέσεων εναντίον συστημάτων πληροφοριών. Οι επιθέσεις εναντίον συστημάτων πληροφοριών μπορεί συχνά να είναι υπερδιεθνής στην φύση τους, και θα απαιτούσαν διεθνή αστυνόμευση και δικαιοσύνη. Η προσέγγιση των νόμων θα βελτιώσει αυτή την συνεργασία εξασφαλίζοντας ότι η ανάγκη διπλής

εγκληματικότητας έχει εκπληρωθεί (στην οποία μια δραστηριότητα πρέπει να είναι αδίκημα σε δύο χώρες πριν κοινή νόμιμη βοήθεια μπορέσει να εξασφαλίσει βοήθεια σε μια έρευνα εγκλήματος). Αυτό θα οδηγήσει τις χώρες μέλη της ευρωπαϊκής ένωσης σε συνεργασία μεταξύ τους, όπως επίσης και στην βελτίωση της συνεργασίας τους με τρίτες χώρες(εξασφαλίζοντας ότι υπάρχει συμφωνία σε έναν κοινό νόμο).

Αυτή η πρόταση επίσης αναπτύσσει μέρος της συνεισφοράς της Ευρωπαϊκής Ένωσης στην ανταπόκριση της απειλής ενός τρομοκρατικού χτυπήματος εναντίον συστημάτων ζωτικών πληροφοριών στην Ε.Ε. Συμπληρώνει τις προτάσεις της Ε.Ε για να αντικαταστήσει τις εκδόσεις υποδίκων εντός της Ε.Ε με ένα ευρωπαϊκό ένταλμα σύλληψης και να προσεγγίσει νόμους πάνω στην τρομοκρατία. Αυτά τα νομικά έγγραφα θα διασφαλίσουν ότι τα κράτη μέλη της Ευρωπαϊκής Ένωσης έχουν αποτελεσματικούς νόμους ώστε να καταπολεμήσουν την ηλεκτρονική τρομοκρατία, και να δυναμώσουν την διεθνή συνεργασία ενάντια στην τρομοκρατία.

Αυτή η πρόταση δεν έχει σχέση μόνο με ενέργειες που γίνονται στα κράτη μέλη. Απευθύνεται επίσης στην καταγραφή της τρομοκρατίας της Ε.Ε , η οποία κατευθύνεται εναντίον συστημάτων πληροφοριών στο έδαφος τρίτων χωρών. Αυτό αναδιπλώνει την δέσμευση της Ένωσης στο να καταπολεμήσει τις επιθέσεις εναντίον συστημάτων πληροφόρησης εξίσου καλά όπως στο επίπεδο της Ε.Ε.

Είναι γεγονός, ότι υπήρξαν ήδη μερικές πρόσφατες υποθέσεις όπου οι εντάσεις στις διεθνείς σχέσεις είχαν οδηγήσει σε ένα δυνατό ξέσπασμα επιθέσεων εναντίον συστημάτων πληροφοριών, συχνά περιλαμβάνοντας επιθέσεις εναντίον ιστοσελίδων. Οι περισσότερες από τις σοβαρές επιθέσεις δεν μπορούσαν μόνο να οδηγήσουν σε σοβαρή οικονομική ζημιά αλλά, σε κάποιες περιπτώσεις, μπορούσαν ακόμη να οδηγήσουν και στην απώλεια μιας ζωής(π.χ. νοσοκομειακά συστήματα, συστήματα ελέγχου εναέριας κυκλοφορίας κ.τ.λ).

2. 1 ΑΣΦΑΛΕΙΑ

Τα τελευταία χρόνια , το INTERNET έχει γίνει ένα μεγάλο super market , όπου πωλούνται όλων των ειδών τα αγαθά. Για να ανθίσει το ηλεκτρονικό εμπόριο όμως , πρέπει οι χρήστες να αισθάνονται ασφαλείς όταν μεταδίδουν μέσω του δικτύου τον αριθμό της πιστωτικής τους κάρτας ή άλλες προσωπικές πληροφορίες οικονομικού περιεχομένου . Επειδή οι πληροφορίες που μεταφέρονται περνάνε από ένα μεγάλο αριθμό υπολογιστών πριν φτάσουν στον προορισμό τους , υπάρχει η δυνατότητα να κλαπούν από κάποιον. Λόγω της τεράστιας δυναμικής που έχει το ηλεκτρονικό εμπόριο , πολλές εταιρείες ξοδεύουν χρόνο και χρήμα έτσι ώστε να προστατεύσουν τις συναλλαγές με τους πελάτες τους .

Αυτό γίνεται με μία μέθοδο που ονομάζεται encryption. Η δουλειά που κάνει το software αυτό είναι να διαβάζει τις πληροφορίες από τον υπολογιστή και να τις μεταβάλλει μέσω ενός μυστικού κώδικα , έτσι ώστε να μην μπορούν να αποκρυπτογραφηθούν από πιθανούς κλέφτες στον δρόμο για τον προορισμό τους .Όταν φτάσουν εκεί , ένα παρόμοιο software αποκωδικοποιεί το σήμα και παίρνει τις αρχικές πληροφορίες . Το πρόβλημα είναι ότι δεν υπάρχει κώδικας ο οποίος να μην μπορεί να «σπαστεί» .

Οι λεγόμενοι hackers είναι άνθρωποι που έχουν σαν ασχολία να σπάζουν τα συστήματα ασφάλειας των υπολογιστών .Πάντως , σε μία σύνδεση μέσω modem , η πιθανότητα να εμπλακεί ένας hacker είναι ιδιαίτερα χαμηλή . Οι αληθινοί στόχοι τους είναι κυρίως εμπορικοί και κυβερνητικοί υπολογιστές .Οι υπολογιστές αυτοί όμως προφυλάσσονται χρησιμοποιώντας firewalls , τα οποία είναι περίπλοκα συστήματα ασφαλείας και βρίσκονται μεταξύ του υπολογιστή και του Internet .

Όλες οι οικονομικές συναλλαγές οφείλουν να είναι ασφαλείς . Πολλά ηλεκτρονικά μαγαζιά έχουν μία 'ασφαλή σελίδα' (secure page) και υπάρχουν τα κατάλληλα links σε αυτές . Επίσης , στον web server υπάρχει ένα εικονίδιο στο κάτω μέρος του παραθύρου , το οποίο είναι συνήθως μία κλειδαριά , που δείχνει αν η σελίδα που παρουσιάζεται εκείνη την στιγμή υποστηρίζει κάποιο είδος ασφάλειας . Άλλες εταιρείες , δίνουν στις σελίδες τους συγκεκριμένα τηλεφωνικά νούμερα όπου ο πελάτης παίρνει και δίνει τις πληροφορίες του μέσω τηλεφώνου . Βέβαια , ούτε οι τηλεφωνικές συνδιαλέξεις είναι 100% ασφαλείς .

Τα ρίσκα που υπάρχουν στο ηλεκτρονικό εμπόριο , δεν είναι μεγαλύτερα από αυτά που αντιμετωπίζονται σε άλλου είδους συναλλαγές

.Πάντως , παρόλο που οι αγορές μέσω Internet θεωρούνται αρκετά ασφαλείς , υπάρχουν πολλές εταιρείες που συνεχίζουν να δουλεύουν στην κατεύθυνση της ανάπτυξης ή της βελτίωσης της τεχνολογίας που θα κάνει το web πιο ασφαλές .

2.2 Το «Σκουλήκι» του Internet

Η μεγαλύτερη παραβίαση ασφαλείας όλων των εποχών σε υπολογιστές ξεκίνησε το απόγευμα της 2ας Νοεμβρίου 1988 , όταν ένας τελειόφοιτος του Πανεπιστημίου Cornell ελευθέρωσε το πρόγραμμα «σκουλήκι» (worm) μέσα στο δίκτυο Internet. Αυτή η πράξη είχε ως αποτέλεσμα να καταρρεύσουν χιλιάδες υπολογιστές σε πανεπιστήμια , εταιρείες και κυβερνητικά εργαστήρια σε ολόκληρο τον κόσμο , προτού αποκαλυφθεί και απομακρυνθεί το « σκουλήκι» .

Το «σκουλήκι» εκμεταλλευόταν ένα σφάλμα που είχε τότε το λειτουργικό Berkeley UNIX , χάρη στο οποίο του επιτρεπόταν να έχει μη εξουσιοδοτημένη πρόσβαση σε υπολογιστές οι οποίοι ήταν συνδεδεμένοι στο Internet . Από την στιγμή που αποκτούσε πρόσβαση σε ένα νέο υπολογιστή αναπαραγόταν σε αυτόν (αντέγραφε τον εαυτό του) και το αντίγραφο του έψαχνε με την σειρά του να αποκτήσει πρόσβαση σε άλλους υπολογιστές κ.ο.κ. Τίποτα όμως στον κώδικα του «σκουληκιού» δεν υποδήλωνε προσπάθεια για να κλέψει ή να χαλάσει οτιδήποτε στους υπολογιστές που αποκτούσε πρόσβαση . Δεν είναι βέβαια γνωστό αν η μορφή που είχε το πρόγραμμα στις 2 Νοεμβρίου 1988 προοριζόταν απλώς για έλεγχο και ξέφυγε στο Internet κατά λάθος ή ήταν η τελική .Γεγονός πάντως είναι ότι οι «μολυσμένοι» υπολογιστές μετά από κάποιο διάστημα κατακλύζονταν από αντίγραφα του «σκουληκιού» και δεν μπορούσαν να λειτουργήσουν .

2.3 Ιοί

Μια ειδική κατηγορία επιθέσεων είναι οι ιοί (viruses) των υπολογιστών , οι οποίοι έχουν γίνει ένα μεγάλο πρόβλημα για πολλούς από τους χρήστες υπολογιστών . Ένας ιός είναι ένα κομμάτι προγράμματος το οποίο επισυνάπτεται σε ένα νομότυπο πρόγραμμα με σκοπό να «μολύνει» άλλα προγράμματα . Διαφέρει από το «σκουλήκι» μόνο στο ότι ένας ιός προσκολλάται σε ένα ήδη υπάρχον πρόγραμμα ενώ

το «σκουλήκι» είναι από μόνο του ένα πλήρες πρόγραμμα . Τόσο οι ιοί , όσο και τα σκουλήκια προσπαθούν να διαδοθούν και μπορούν να προκαλέσουν σοβαρές ζημιές .

Αυτός που γράφει έναν ιό συνήθως γράφει ένα χρήσιμο πρόγραμμα , όπως ένα παιχνίδι για MS-DOS και τοποθετεί μέσα του τον κώδικα του ιού . Στη συνέχεια το πρόγραμμα μεταφέρεται σε κάποιο Web site ή προσφέρεται δωρεάν ή σε κάποια χαμηλή τιμή σε δισκέτα .Στη συνέχεια το πρόγραμμα διαφημίζεται , οπότε οι άνθρωποι αρχίζουν να το μεταφέρουν στους υπολογιστές τους και να το χρησιμοποιούν .

Όταν το πρόγραμμα του ιού ξεκινάει , αρχίζει αμέσως να εξετάζει όλα τα εκτελέσιμα προγράμματα στον σκληρό δίσκο για να δει αν έχουν ήδη μολυνθεί . Όταν βρει ένα μη μολυσμένο πρόγραμμα , το μολύνει επισυνάπτοντας τον κώδικα του ιού στο τέλος του αρχείου . Με τον τρόπο αυτό , κάθε φορά που ένα μολυσμένο πρόγραμμα εκτελείται προσπαθεί να μολύνει και άλλα προγράμματα . Εκτός όμως από το να αντιγράψει τον εαυτό του ένας ιός μπορεί να κάνει και πολλά άλλα πράγματα , όπως να διαγράψει , να αλλάξει ή να κρυπτογραφήσει αρχεία .Υπήρξε ένα ιός που παρουσίαζε στην οθόνη ένα εκβιαστικό μήνυμα , το οποίο ζητούσε από τον χρήστη να στείλει 500 δολάρια μετρητά σε μία ταχυδρομική θυρίδα στον Παναμά , διαφορετικά θα έχανε για πάντα όλα τα δεδομένα του !!

2.4 Απειλές στο World Wide Web

Το World Wide Web είναι ίσως το γρηγορότερα αναπτυσσόμενο κομμάτι του Internet . Ολοένα όμως και περισσότερο γίνεται και το κομμάτι του Internet που είναι πιο ευάλωτο σε επιθέσεις . Οι υπολογιστές που φιλοξενούν ιστοσελίδες (web servers) αποτελούν ελκυστικούς στόχους για πολλούς λόγους :

- Δημοσιότητα : Οι ιστοσελίδες ενός οργανισμού ή μιας επιχείρησης αποτελούν την εικόνα του στον υπόλοιπο κόσμο του Internet . Μια επιτυχημένη επίθεση σε έναν web server μπορεί να αλλάξει πληροφορίες σε ιστοσελίδες που βλέπουν εκατοντάδες χιλιάδες ανθρώπων μέσα σε μερικές ώρες και είτε να προπαγανδίσει

διαφορετικές φιλοσοφίες ή ιδεολογίες ή απλώς να χαλάσει τη δημόσια εικόνα του θύματος .

❖ Εμπόριο : Πολλές ιστοσελίδες περιέχουν φόρμες για την αγορά αγαθών ή την πραγματοποίηση άλλων εμπορικών συναλλαγών (π.χ. πληρωμή προστίμων στην τροχαία) . Οι συναλλαγές αυτές γίνονται συνήθως μέσω της ανταλλαγής πληροφοριών που περιλαμβάνουν τα στοιχεία κάποιας πιστωτικής κάρτας του χρήστη , κάτι που κάνει αυτούς τους υπολογιστές στόχους επιθέσεων με σκοπό την υποκλοπή αυτών των πληροφοριών .

❖ «Εσωτερικές» Πληροφορίες : Πολλές επιχειρήσεις χρησιμοποιούν το World Wide Web για να μεταδώσουν πληροφορίες στα μέλη τους ή σε άλλους συνεργάτες τους στο εξωτερικό . Οι πληροφορίες αυτές , όπως είναι φυσικό , αποτελούν στόχο των εμπορικών ανταγωνιστών ή εχθρών τους .

❖ Πρόσβαση σε δίκτυα : Επειδή οι υπολογιστές που φιλοξενούν ιστοσελίδες κάποιας επιχείρησης χρησιμοποιούνται και από τους εργαζόμενους μέσα στην επιχείρηση αλλά και από τον υπόλοιπο κόσμο του Internet , αποτελούν μία γέφυρα επικοινωνίας ανάμεσα στο Internet και στα διάφορα τοπικά δίκτυα των επιχειρήσεων . Επομένως η θέση τους , τους κάνει ιδανικούς στόχους επίθεσης ώστε στη συνέχεια να αποτελέσουν «ορμητήρια» των εισβολέων στο εσωτερικό δίκτυο της επιχείρησης .

❖ Οι απειλές στο World Wide Web χωρίζονται σε τρεις κατηγορίες :

1. *Απειλές κατά του web server*
2. *Απειλές κατά την μεταφορά των δεδομένων και κατά αποθηκευμένων δεδομένων* κυρίως όταν πρόκειται για αριθμούς πιστωτικών καρτών ή άλλες ευαίσθητες πληροφορίες εμπορικών επιχειρήσεων ή στρατιωτικών οργανώσεων .

3. *Απειλές κατά του υπολογιστή του χρήστη* μέσω προβλημάτων που πολλές φορές υπάρχουν στον κώδικα του προγράμματος που χρησιμοποιεί ο χρήστης για την ανάγνωση των ιστοσελίδων (π.χ. Microsoft Internet Explorer , Netscape Navigator) .

2.5 Προστασία από Δούρειους Ίππους

Βασικός τρόπος προστασίας από τέτοιου είδους απειλές είναι η χρήση μηχανισμού ελεγχόμενης πρόσβασης των αρχείων με ταυτόχρονο έλεγχο των μεγεθών και των ημερομηνιών αλλαγής των αρχείων που περιέχουν τα προγράμματα που εκτελούνται στο σύστημα (audit) . Επίσης , ο κάθε χρήστης προστατεύεται αν ο ίδιος κάνει έναν έλεγχο των προγραμμάτων τα οποία κάθε φορά εκτελεί έτσι ώστε να μην εκτελεστεί το πρόγραμμα κάποιου εισβολέα στη θέση του επιθυμητού προγράμματος .

2.6 Προστασία από «σκουλήκια» και ιούς

Προστασία από τέτοιου είδους απειλές παρέχει η χρήση μηχανισμού ελεγχόμενης πρόσβασης των αρχείων και η αποφυγή μετάδοσης κάποιου ιού ή «σκουληκιού» στο σύστημα μέσω της εκτέλεσης κάποιου «μολυσμένου» προγράμματος . Οι χρήστες επομένως πρέπει να αποφεύγουν την εκτέλεση προγραμμάτων άγνωστης ή αμφιβόλου προελεύσεως που βρέθηκαν στα χέρια τους τυχαία , πιθανόν από κάποιο web site ή κάποιο ανώνυμο ftp site , ή τους στάλθηκαν ως attachments μέσω του ηλεκτρονικού ταχυδρομείου (email) από αγνώστους ή ανύπαρκτους χρήστες .

Στην περίπτωση που παρά την προσεκτική επιλογή των προγραμμάτων που εγκαθίστανται σε έναν υπολογιστή ο υπολογιστής αυτός προσβληθεί από κάποιον ιό υπάρχουν ειδικά

«αντιβιοτικά» προγράμματα (antivirus) τα οποία μπορούν να ψάξουν σε όλους τους χώρους αποθήκευσης του υπολογιστή , να εντοπίσουν γνωστούς ιούς και να τους σβήσουν . Πολλά μάλιστα από αυτά τα προγράμματα μπορούν να ελέγχουν συνεχώς τον υπολογιστή κατά την ώρα εργασίας και να ειδοποιούν μόλις εντοπίσουν κάποιο προγραμματιστικό κώδικα ιού ώστε να είναι δυνατή η έγκαιρη «θεραπεία» του υπολογιστή πριν δράσει ο ιός και προσβάλλει τις πληροφορίες που είναι αποθηκευμένες . Τέτοια προγράμματα είναι το Norton Antivirus που είναι αγορασμένο από το Κέντρο Υπολογιστών του Πανεπιστημίου , το McAfee Virus Scan που διατίθεται σε διάφορα Web sites (π.χ. http://www. Tucows . gr/) και άλλα .

Βέβαια , τα προγράμματα αυτά μπορούν να ανιχνεύσουν μόνο γνωστούς ιούς , δηλαδή ιούς που έχουν κάνει την εμφάνιση τους παλαιότερα και έχουν καταγραφεί , ενώ είναι ανίσχυρα εναντίον νέων πρωτοεμφανιζόμενων ιών . Για αυτό το λόγο οι εταιρείες που τα κατασκευάζουν διαθέτουν συνεχώς στους χρήστες τους αναβαθμίσεις ώστε να μπορούν τα προγράμματα αυτά να προστατεύουν και από τους ιούς που έκαναν την εμφάνιση τους πρόσφατα .

2.7 Προστασία από απειλές του World Wide Web

Η στρατηγική για να προστατευτεί ο web server από ενδεχόμενες εισβολές είναι ο περιορισμός των υπηρεσιών που παρέχει ο υπολογιστής αυτός πέραν του Web σε όσο γίνεται λιγότερες . Επίσης , καλή στρατηγική είναι και ο περιορισμός των χρηστών που έχουν λογαριασμό (account) σε αυτόν τον υπολογιστή , ενώ αυτοί που έχουν λογαριασμό και επικοινωνούν με τον υπολογιστή αυτό από μακριά πρέπει να χρησιμοποιούν κάποιο ασφαλές πρόγραμμα επικοινωνίας (π.χ. Kerberised Telnet , ssh) .

Για να προστατευτούν οι πληροφορίες κατά τη μεταφορά τους μέσω του World Wide Web ακολουθείται η στρατηγική της κρυπτογράφησης . Ένα τέτοιο σύστημα κρυπτογράφησης δεδομένων που στέλνονται μέσω

του World Wide Web είναι το Secure Socket Layer (SSL) και θα πρέπει οι χρήστες να το χρησιμοποιούν κάθε φορά που στέλνουν ευαίσθητες πληροφορίες .

Τέλος , απειλές στο World Wide Web προέρχονται και από προγράμματα που εκτελούνται άμεσα από τα προγράμματα ανάγνωσης των ιστοσελίδων (browsers) , όπως προγράμματα Java , JavaScript , ActiveX κ.τ.λ. ή από την χρήση των λεγόμενων cookies . Αν και τέτοια προγράμματα δίνουν ζωή στις ιστοσελίδες του World Wide Web εντούτοις μπορούν να αποτελέσουν πολύ επικίνδυνα όπλα στα χέρια πιθανών εισβολέων οι οποίοι θα εκμεταλλευτούν λάθη στην κατασκευή των browsers ώστε να μπορέσουν να προκαλέσουν ζημιά ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε διάφορους υπολογιστές . Προστασία από τέτοιες απειλές παρέχουν τα ίδια τα προγράμματα ανάγνωσης ιστοσελίδων (browsers) μέσα από επιλογές για απενεργοποίηση της δυνατότητας εκτέλεσης τέτοιων δυναμικών προγραμμάτων ανάλογα με την προέλευσή τους .

2.8 Κατηγορίες επιθέσεων και μοντέλα ασφαλείας

Μέσω των χρόνων, πολλοί διαφορετικοί τύποι επιθέσεων σε κρυπτογραφικά πρωτόκολλα έχουν αναγνωρισθεί. Παρακάτω θα δούμε τις αιτίες των επιθέσεων στην απόκρυψη και στα πρωτόκολλα. Οι επιθέσεις μπορούν να διαχωριστούν ως εξής:

1. Η παθητική επίθεση είναι αυτή όπου μόνο ο εχθρός παρακολουθεί το κανάλι επικοινωνίας. Ένας παθητικός επιτιθέμενος απειλεί μόνο εμπιστευτικές πληροφορίες.
2. Μια ενεργή επίθεση είναι αυτή όπου ο εχθρός προσπαθεί να διαγράψει, να προσθέσει, ή κατά έναν άλλο τρόπο να αλλάξει την μετάδοση του καναλιού. Ένας ενεργός επιτιθέμενος απειλεί ακέραιες πληροφορίες και πιστοποιημένες.

2.8.1 Επιθέσεις σε μεθόδους απόκρυψης

Το αντικείμενο των ακόλουθων επιθέσεων είναι η συστηματική επανάκτηση μη κωδικοποιημένων κειμένων από κρυπτογραφία, ή ακόμη πιο δραστικά, η αποκάλυψη του κλειδιού της απόκρυψης.

1. Μια κρυπτογραφημένη μόνο επίθεση είναι όπου ο εχθρός(ή κρυπταναλυτής) προσπαθεί να βρει το κλειδί της απόκρυψης ή να το αποκωδικοποιήσει παρατηρώντας την κρυπτογραφία. Οποιαδήποτε μέθοδος απόκρυψης ευαίσθητη σε αυτόν τον τύπο της επίθεσης είναι ολοκληρωτικά ανασφαλής.
2. Μια γνωστή μη κωδικοποιημένη επίθεση είναι όπου ο εχθρός έχει μια ποσότητα μη κωδικοποιημένων και σχετικών κρυπτογραφημάτων. Αυτός ο τύπος επιθέσεων είναι τυπικά οριακά πιο δύσκολος να υπολογισθεί.
3. Μια επιλεγμένη μη κωδικοποιημένη επίθεση είναι όπου ο εχθρός επιλέγει μη κωδικοποιημένα κείμενα και μετά δίνονται σχετικά κρυπτογραφήματα. Μετέπειτα, ο εχθρός χρησιμοποιεί οποιαδήποτε πληροφορία για να ανακτήσει μη κωδικοποιημένα κείμενα σχετικά με προηγούμενα άγνωστα κρυπτογραφήματα.
4. Μια προσαρμόσιμη επιλεγμένη μη κωδικοποιημένη επίθεση είναι μια επιλεγμένη μη κωδικοποιημένη επίθεση όπου η επιλογή ενός μη κωδικοποιημένου μηνύματος μπορεί να βασίζεται σε ένα κρυπτογράφημα που έχει φτάσει από προηγούμενους αιτήσεις.
5. Μια επιλεγμένη κρυπτογραφημένη επίθεση είναι όπου ο εχθρός επιλέγει το κρυπτογράφημα. Ένας τρόπος να υπολογισθεί μια τέτοια επίθεση είναι κερδίζοντας ο εχθρός πρόσβαση στον εξοπλισμό που χρησιμοποιείται για αποκωδικοποίηση.
6. Μια προσαρμοσμένη επιλεγμένη επίθεση είναι όπου η επιλογή του κρυπτογραφήματος μπορεί να βασίζεται σε ένα μη

κωδικοποιημένο κείμενο που μόλις έχει φθάσει από προηγούμενες αιτήσεις.
Οι περισσότερες από αυτές τις επιθέσεις απευθύνονται επίσης σε μεθόδους ψηφιακών υπογραφών και σε κώδικες μηνυμάτων πιστοποίησης. Σε αυτήν την περίπτωση το αντικείμενο του επιτιθέμενου είναι να παραποιήσει μηνύματα.

2.8.2 Επιθέσεις σε πρωτόκολλα

Τα παρακάτω είναι μια μονομερή λίστα επιθέσεων που εξαπολύθηκαν σε διάφορα πρωτόκολλα. Μέχρις ότου ένα πρωτόκολλο είναι αρχή διασφάλισης υπηρεσιών, η λίστα των πιθανών επιθέσεων δεν μπορεί να ειπωθεί ότι έχει ολοκληρωθεί.

1. Γνωστό κλειδί επίθεσης. Σε αυτήν την επίθεση ένας εχθρός αποκτά κάποια κλειδιά που προηγούμενα χρησιμοποιήθηκαν και μετά χρησιμοποιεί αυτήν την πληροφορία για να ορίσει καινούρια κλειδιά.
2. Επανάληψη. Σε αυτήν την επίθεση ένας εχθρός καταγράφει μια περίοδο επικοινωνίας και επαναλαμβάνει ολόκληρη την περίοδο, ή ένα μέρος αυτής, σε ένα μετέπειτα χρονικό σημείο.
3. Προσωποποίηση. Εδώ ένας εχθρός παίρνει την ταυτότητα ενός από τις νόμιμες ομάδες μέσα σε ένα δίκτυο.
4. Λεξικό. Αυτή είναι συνήθως μια επίθεση εναντίον των passwords. Τυπικά το password είναι αποθηκευμένο σε έναν φάκελο ενός υπολογιστή όπως η εικόνα μιας μπερδεμένης λειτουργίας. Όταν ένας χρήστης χρεώνεται και βάζει το password, αυτό μπερδεύεται. Ένας εχθρός μπορεί να πάρει μια λίστα πιθανόν passwords, να ανακατέψει όλες τις καταχωρήσεις στην λίστα αυτή, και μετά να τις συγκρίνει με μια λίστα αληθινών passwords με την ελπίδα να βρει αντιστοιχίσεις.
5. Προωθημένη έρευνα. Αυτή η επίθεση είναι ίδια στο πνεύμα με αυτήν του λεξικού και χρησιμοποιείται για αποκωδικοποίηση μηνυμάτων.
6. Επίθεση από στρώμα σε στρώμα. Αυτός ο τύπος επίθεσης συνήθως περιλαμβάνει μερικά πρότυπα προσωποποίησης σε ένα πρωτόκολλο πιστοποίησης.

2.8.3 Μοντέλα αξιολογημένης ασφάλειας

Η ασφάλεια των κρυπτογραφημάτων και των πρωτοκόλλων μπορεί να αξιολογηθεί κάτω από διαφορετικά μοντέλα. Τα πιο πρακτικά μοντέλα ασφαλείας είναι το υπολογιστικό, το αποδεικτό, και η μεθοδολογία αναφερόμενη σε ειδικό σκοπό, αν και η τελευταία είναι συχνά επικίνδυνη. Το επίπεδο εμπιστοσύνης, στην ποσότητα που η ασφάλεια παρέχεται από πρωτόκολλο βασισμένο στην υπολογιστική ή στην αναφερόμενη σε ειδικό σκοπό ασφάλεια, αυξάνεται με τον χρόνο και την έρευνα της μεθόδου. Ωστόσο, ο χρόνος δεν είναι αρκετός αν μερικοί άνθρωποι έχουν δώσει στην μέθοδο προσεκτική ανάλυση.

(i) Απεριόριστη ασφάλεια

Το πιο άκαμπτο μέτρο είναι ένα θεωρητικό-πληροφοριακό μέτρο, όπου ένα σύστημα έχει ή δεν έχει απεριόριστη ασφάλεια. Ένας εχθρός προσπαθεί να έχει απεριόριστους υπολογιστικούς πόρους, και η ερώτηση είναι αν υπάρχει αρκετή πληροφόρηση διαθέσιμη για να νικήσει το σύστημα. Απεριόριστη ασφάλεια για συστήματα απόκρυψης ονομάζεται τέλεια μυστικότητα. Για τέλεια μυστικότητα, η αστάθεια στο μη κωδικοποιημένο μήνυμα, αφού παρατηρώντας το κρυπτογράφημα, πρέπει να είναι ίση με μια πρώτιστη αστάθεια για το μη κωδικοποιημένο μήνυμα.
Μια απαραίτητη κατάσταση για μια απόκρυψη συμμετρικού κλειδιού μοιάζει να είναι απεριόριστα ασφαλής έτσι ώστε το κλειδί να είναι τουλάχιστον όσο μεγάλο όσο το μήνυμα. Το one-time pad είναι ένα παράδειγμα ενός απεριόριστα ασφαλούς αλγορίθμου απόκρυψης. Γενικά, οι μέθοδοι απόκρυψης δεν προσφέρουν τέλεια μυστικότητα, όπως επίσης και ο κάθε χαρακτήρας κρυπτογραφήματος και το κλειδί απόκρυψης. Οι μέθοδοι απόκρυψης δημόσιου κλειδιού δεν μπορούν να έχουν απεριόριστη ασφάλεια.

(i) Πολύπλοκη-θεωρητική ασφάλεια

Ένα κατάλληλο υπολογιστικό μοντέλο ορίζεται και οι εχθροί μοντελοποιούνται καθώς έχουν πολυωνυμική υπολογιστική δύναμη.(Εξαπολύουν επιθέσεις περιλαμβάνοντας πολυωνυμικό χρόνο και χώρο στο μέγεθος κατάλληλων παραμέτρων ασφάλειας.) Μια απόδειξη ασφάλείας που σχετίζεται με το μοντέλο κατασκευάζεται μετά. Αντικειμενικός σκοπός είναι να σχεδιαστεί μια κρυπτογραφική μέθοδος βασισμένη στις πιο

αδύναμες προϋποθέσεις προβλέποντας πιθανώς έναν δυνατό εχθρό. Ασύμπτωτες αναλύσεις και συχνά επίσης χειρότερες ως προς την περίπτωση αναλύσεις χρησιμοποιούνται ώστε να πρέπει να εξασκούνται για να ορίζουν όταν οι δοκιμές έχουν πρακτικό νόημα. Επιπλέον, οι πολυωνυμικές επιθέσεις οι οποίες είναι εφικτές μέσω του μοντέλου μπορεί, στην εφαρμογή, να είναι ακόμη υπολογιστικά μη εφικτές.

Αναλύσεις ασφάλειας αυτού του τύπου, αν και δεν είναι πρακτικής έννοιας σε κάθε περίπτωση, παρ'όλα αυτά μπορεί να προετοιμάζουν τον δρόμο για μια καλύτερη συνολικά κατανόηση της ασφάλειας. Οι πολύπλοκες θεωρητικά αναλύσεις είναι ανεκτίμητες για την διατύπωση θεμελιωδών αρχών και την επιβεβαίωση ιδεών. Αυτό είναι όπως πολλές άλλες επιστήμες, των οποίων οι πρακτικές τεχνικές ανακαλύφθηκαν νωρίτερα στην εξέλιξη, πριν καλά φανεί μια θεωρητική βάση και κατανόηση.

(iii) Αποδεικτέα ασφάλεια

Μια κρυπτογραφική μέθοδος λέγεται ότι είναι αποδεικτά ασφαλής αν η δυσκολία της εφαρμογής της μπορεί να φαίνεται ότι είναι ουσιωδώς δύσκολη όπως λύνοντας ένα γνώριμο και δήθεν δύσκολο πρόβλημα, όπως την παραγοντοποίηση ενός ακέραιου αριθμού ή τον υπολογισμό ξεχωριστών αλγόριθμων.

Η αποδεικτέα ασφάλεια μπορεί να φαίνεται μέρος μιας ειδικής υποκλάσης της μεγαλύτερης κλάσης μοντέλων υπολογιστικής ασφάλειας.

(iv) Υπολογιστική ασφάλεια

Αυτό μετρά την ποσότητα της υπολογιστικής ενέργειας που απαιτείται, από τις καλύτερες επι του παρόντος γνωστές μεθόδους, για να νικήσει το σύστημα. Μια προτεινόμενη τεχνική λέγεται ότι είναι υπολογιστικά ασφαλής εάν το προβλεπόμενο επίπεδο υπολογισμού που απαιτήται για να νικήσει το σύστημα υπερβαίνει τους υπολογιστικούς πόρους των υποτιθέμενων εχθρών.

Συχνά μέθοδοι της κλάσης αυτής σχετίζονται με δύσκολα προβλήματα αλλά, διαφορετικά για αποδεικτέα ασφάλεια, καμία απόδειξη ισοδυναμίας είναι γνωστή. Οι περισσότερες από τις πιο γνωστές μεθόδους δημόσιου και συμμετρικού κλειδιού σε τρέχουσα χρήση είναι σε αυτήν την κλάση. Αυτή η κλάση μερικές φορές επίσης ονομάζεται πρακτική ασφάλεια.

3.1 Κρυπτογράφηση

Το διαδίκτυο ήδη χρησιμοποιείται από εκατομμύρια χρήστες και επεκτείνεται με εκθετικούς ρυθμούς αύξησης . Μπορεί να θεωρηθεί ένας χώρος επικοινωνίας , εκπαίδευσης και οικονομικής δραστηριότητας με διαρκώς αυξανόμενη δύναμη . Η νέα αυτή ψηφιακή κοινωνία οφείλει να παρέχει μηχανισμούς προστασίας του απαραβίαστου της προσωπικής ζωής των μελών της , το οποίο αποτελεί θεμελιώδες ανθρώπινο δικαίωμα .

Σε νομικό και κοινωνικό επίπεδο , τίθεται ζήτημα προστασίας του απορρήτου της ηλεκτρονικής αλληλογραφίας (e-mail) , των συναλλαγών (αριθμός πιστωτικής κάρτας , τραπεζικό απόρρητο) , του ιατρικού απορρήτου και γενικότερα το ζήτημα της προστασίας προσωπικών στοιχείων και δεδομένων του κάθε χρήστη του Διαδικτύου , που με διάφορους τρόπους μπορούν να συλλεχθούν από τρίτους και να χρησιμοποιηθούν για οποιονδήποτε σκοπό χωρίς την συγκατάθεση του .

Σε ακαδημαικό επίπεδο , τίθεται θέμα προστασίας αποτελεσμάτων ακαδημαικής έρευνας , ευαίσθητων προσωπικών δεδομένων (βαθμολογία φοιτητών) , ακαδημαικών μελετών και γενικότερα προστασίας των πνευματικών δικαιωμάτων (copyright) των μελών της ακαδημαικής κοινότητας .

Σε οικονομικό επίπεδο , η ασφάλεια και προστασία των εμπορικών πλέον δεδομένων , όπως η εξασφάλιση της εγκυρότητας των συναλλαγών μέσω της αποδοχής μίας ηλεκτρονικής υπογραφής και η ασφάλεια των συναλλαγών είναι κρίσιμα ζητήματα , που αποτελούν το υπόβαθρο της ψηφιακής παγκόσμιας αγοράς .

Το Internet ,λοιπόν , ως μία κουλτούρα ανοιχτή , δωρεάν και ελεύθερη με διάφορες μετεξελίξεις και βελτιώσεις , όπως η εισαγωγή της ισχυρής κρυπτογραφίας , έτσι ώστε να μην μπορούν οι ισχυροί και το αστυνομικό κράτος να κρυφοκοιτούν τους πολίτες . Με την ισχυρή κρυπτογραφία θα επιτευχθεί η προστασία της ατομικής ζωής και της επικοινωνίας των πολιτών .

Η κρυπτογραφία είναι αυτή που εξασφαλίζει το απόρρητο των προσωπικών πληροφοριών και είναι η τεχνολογική πλευρά της λύσης στα προαναφερθέντα ζητήματα ασφαλείας .

3.2 Βασικές έννοιες της κρυπτογραφίας

Η κρυπτογραφία είναι μια επιστήμη που βασίζεται στα μαθηματικά για την κωδικοποίηση και αποκωδικοποίηση των δεδομένων . Οι μέθοδοι κρυπτογράφησης καθιστούν τα ευαίσθητα προσωπικά δεδομένα προσβάσιμα μόνο από όσους είναι κατάλληλα εξουσιοδοτημένοι . Εξασφαλίζουν έτσι το απόρρητο στις ψηφιακές επικοινωνίες αλλά και στην αποθήκευση ευαίσθητων πληροφοριών . Το αρχικό μήνυμα ονομάζεται απλό κείμενο (plaintext) , ενώ το ακατάληπτο μήνυμα που προκύπτει από την κρυπτογράφηση του απλού κειμένου ονομάζεται κρυπτογράφημα (ciphertext) .

Αποκρυπτογράφηση είναι η ανάκτηση του απλού κειμένου από το κρυπτογράφημα με την εφαρμογή αντίστροφου αλγορίθμου . Η κρυπτογραφημένη επικοινωνία είναι αποτελεσματική , όταν μόνο τα άτομα που συμμετέχουν σε αυτή μπορούν να ανακτήσουν το περιεχόμενο του αρχικού μηνύματος .

Η κρυπτογραφία δεν πρέπει να συγχέεται με την κρυπτανάλυση , που ορίζεται ως η επιστήμη για την ανάλυση και αποκωδικοποίηση κωδικοποιημένων πληροφοριών χωρίς την χρήση του αντίστροφου αλγορίθμου κρυπτογράφησης .

Ο αλγόριθμος κρυπτογράφησης είναι μια μαθηματική συνάρτηση που χρησιμοποιείται για την κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών . Όσο αυξάνει ο βαθμός πολυπλοκότητας του αλγορίθμου , τόσο μειώνεται η πιθανότητα να τον διαβάλλει κάποιος . Ο αλγόριθμος κρυπτογράφησης λειτουργεί σε συνδυασμό με ένα κλειδί (key) , για την κρυπτογράφηση του απλού κειμένου . Το ίδιο απλό κείμενο

κωδικοποιείται σε διαφορετικά κρυπτογραφήματα όταν χρησιμοποιούνται διαφορετικά κλειδιά .

Παράδειγμα : Κρυπτογραφικός Αλγόριθμος του Καίσαρα

Ο Ιούλιος Καίσαρας επινόησε έναν απλό κρυπτογραφικό αλγόριθμο για να επικοινωνεί με τους επιτελείς του , με μηνύματα που δεν θα ήταν δυνατόν να τα διαβάσουν οι εχθροί του . Ο αλγόριθμος βασιζόταν στην αντικατάσταση κάθε γράμματος του αλφαβήτου με κάποιο άλλο , όχι όμως τυχαία επιλεγμένο . Ο αλγόριθμος κρυπτογράφησης είναι η ολίσθηση των γραμμάτων του αλφαβήτου προς τα δεξιά . Κάθε γράμμα αντικαθίσταται από κάποιο άλλο με κάποιο κλειδί π.χ. 3 . Δηλαδή , η κρυπτογράφηση ενός μηνύματος γίνεται με αντικατάσταση κάθε γράμματος από το γράμμα που βρίσκεται 3 θέσεις δεξιότερά του στο αλφάβητο . Θα μπορούσε φυσικά το κλειδί να ήταν 6 , οπότε το κρυπτογραφημένο κείμενο που θα προέκυπτε θα ήταν διαφορετικό . Έτσι , διατηρώντας τον ίδιο αλγόριθμο κρυπτογράφησης και επιλέγοντας διαφορετικό κλειδί παράγονται διαφορετικά κρυπτογραφημένα μηνύματα .

Ο πίνακας αντιστοίχισης των γραμμάτων φαίνεται παρακάτω :

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

και πόσες θέσεις χρειάζεται να τα ολισθήσει . Πρέπει να γνωρίζει το κλειδί , που σε αυτήν την περίπτωση είναι ο αριθμός 3 .

3.3 Συμμετρική και ασύμμετρη κρυπτογραφία

Συμμετρική κρυπτογραφία

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

Υπάρχουν αρκετοί αλγόριθμοι που ανήκουν στην κατηγορία αυτή , με περισσότερο γνωστό το Data Encryption Standard (DES) , ο οποίος αναπτύχθηκε αρχικά από την IBM και υιοθετήθηκε το 1977 από την κυβέρνηση των Η.Π.Α. ως το επίσημο πρότυπο κρυπτογράφησης απόρρητων πληροφοριών .

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

Τα σχήματα αυτά παρουσιάζουν το μειονέκτημα ότι δεν είναι εύκολο να επεκταθούν για την εξυπηρέτηση μεγάλων πληθυσμών και απαιτούν

επίσης πρόσθετες διαδικασίες ασφάλειας , όπως την αποθήκευση των κλειδιών σε ένα κεντρικό ασφαλή εξυπηρετητή .

Ασύμμετρη Κρυπτογραφία

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

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

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

Για να αποκατασταθεί επικοινωνία με χρήση ασύμμετρης κρυπτογραφίας , ο κάθε χρήστης πρέπει να διαθέτει τα δικά του κλειδιά ,

---

ένα δημόσιο κλειδί και ένα ιδιωτικό . Ο αποστολέας ενός μηνύματος πρέπει να γνωρίζει το δημόσιο κλειδί του παραλήπτη και να κρυπτογραφήσει το μήνυμα με αυτό . Ο παραλήπτης αποκρυπτογραφεί το μήνυμα με το ιδιωτικό του κλειδί .

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

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

3.4 Ψηφιακές Υπογραφές

Η ασύμμετρη κρυπτογραφία παρέχει τη δυνατότητα πιστοποίησης της αυθεντικότητας ενός μηνύματος , με την παραγωγή μιας μοναδικής ***ψηφιακής υπογραφής*** (digital signature) . Η ψηφιακή υπογραφή είναι μία ακολουθία χαρακτήρων άμεσα συσχετισμένη με το περιεχόμενο του μηνύματος και την ταυτότητα αυτού που το υπογράφει . Αποστέλλεται μαζί με το μήνυμα και ο παραλήπτης μπορεί , ελέγχοντας την υπογραφή , να βεβαιωθεί ότι το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί και ότι ο αποστολέας του είναι όντως αυτός που ισχυρίζεται ότι είναι .

Ο αποστολέας υπογράφει το μήνυμα με το ιδιωτικό του κλειδί . Ο παραλήπτης διαθέτει το δημόσιο κλειδί του αποστολέα και μπορεί να

επιβεβαιώσει ότι το μήνυμα υπογράφτηκε με το αντίστοιχο ιδιωτικό κλειδί . Εφ' όσον το ιδιωτικό κλειδί είναι γνωστό μόνο στον ιδιοκτήτη του , μόνο αυτός θα μπορούσε να το χρησιμοποιήσει , για να υπογράψει

κάποιο μήνυμα και επομένως μόνο αυτός θα μπορούσε να έχει στείλει το μήνυμα αυτό .

Πιο αναλυτικά , πρώτο βήμα για την δημιουργία της ψηφιακής υπογραφής είναι η παραγωγή μιας ***σύνοψης μηνύματος*** (message digest) . Για το σκοπό αυτό , το λογισμικό που παράγει τις υπογραφές χρησιμοποιεί μία ***συνάρτηση κατακερματισμού*** (hash function) . Η συνάρτηση αυτή αντιστοιχεί σε κάθε μήνυμα μία μοναδική ακολουθία χαρακτήρων , που ονομάζεται σύνοψη του μηνύματος και έχει σταθερό μήκος , ανεξάρτητα από το μήκος του μηνύματος . Η σύνοψη , κρυπτογραφημένη με το ιδιωτικό κλειδί του αποστολέα , αποτελεί την υπογραφή , η οποία επισυνάπτεται στο μήνυμα .

Ο παραλήπτης λαμβάνει τόσο το μήνυμα όσο και την υπογραφή . Χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για να αποκρυπτογραφήσει την υπογραφή , οπότε προκύπτει η σύνοψη του μηνύματος , όπως αυτή είχε παραχθεί πριν την αποστολή του μηνύματος . Εφ' όσον η υπογραφή έχει παραχθεί με το ιδιωτικό κλειδί του αποστολέα , μόνο το δημόσιο κλειδί του μπορεί να την αποκρυπτογραφήσει και να δώσει τη σύνοψη του μηνύματος . Η συνάρτηση κατακερματισμού χρησιμοποιείται για να παραχθεί μία σύνοψη του μηνύματος , όπως αυτό έχει φτάσει στα χέρια του παραλήπτη . Εφ' όσον το περιεχόμενο του μηνύματος δεν έχει παραποιηθεί μετά από την αποστολή του , η σύνοψη του μηνύματος θα

είναι ίδια με αυτήν που είχε προκύψει κατά την υπογραφή του από τον αποστολέα . Με αυτόν τον τρόπο , ο παραλήπτης βεβαιώνει την αυθεντικότητα του μηνύματος .

3.5 Υποδομή Δημοσίου Κλειδιού

Η Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure – PKI) είναι ένας συνδυασμός λογισμικού , τεχνολογιών κρυπτογραφίας και υπηρεσιών που επιβεβαιώνουν και πιστοποιούν την εγκυρότητα της κάθε οντότητας που εμπλέκεται σε μια συναλλαγή με το Διαδίκτυο , και παράλληλα προστατεύουν την ασφάλεια της συναλλαγής .

Η Υποδομή Δημοσίου Κλειδιού ενσωματώνει ψηφιακά πιστοποιητικά , κρυπτογραφία δημόσιου κλειδιού και αρχές πιστοποίησης σε ένα ασφαλές αρχιτεκτονικό σχήμα . Μια τυπική υλοποίηση της Υποδομής Δημοσίου Κλειδιού περιλαμβάνει την παροχή ψηφιακών πιστοποιητικών σε χρήστες , σε εξυπηρετητές , σε λογισμικό χρηστών , καθώς επίσης και εργαλείων για την διαχείριση , ανανέωση και ανάκληση των πιστοποιητικών αυτών .

3.5.1 Υπηρεσίες Υποδομής Δημοσίου Κλειδιού

Υπάρχουν οι εξής βασικές λειτουργίες που είναι κοινές σε όλες τις Υποδομές Δημοσίου Κλειδιού και περιγράφονται αναλυτικά στις επόμενες υποενότητες .

Εμπιστευτικότητα (Confidentiality)

Ως εμπιστευτικότητα ορίζεται η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη πρόσβαση ή γνωστοποίηση τους . Η υπηρεσία αυτή υλοποιείται μέσω μηχανισμών ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κωδικοποίησης κατά την αποστολή δεδομένων . Η Υποδομή Δημοσίου Κλειδιού παρέχει κωδικοποίηση , αφού οι μηχανισμοί ελέγχου πρόσβασης υλοποιούνται κατά βάση από τον συνδυασμό μεθόδων πιστοποίησης (authentication) και εξουσιοδότησης (authorization) .

3. Κρυπτογράφηση

Η εμπιστευτικότητα μπορεί να παρομοιασθεί με έναν αδιαφανή φάκελο . Το μήνυμα που περιλαμβάνει δεν είναι ορατό χωρίς να ανοίξει ο φάκελος . Φυσικά , ο φάκελος μπορεί να ανοιχθεί από τον οποιονδήποτε και να παραβιασθεί το απόρρητο της αλληλογραφίας .

Η κρυπτογραφία είναι ένας απολύτως ασφαλής φάκελος που πολύ δύσκολα , σχεδόν ακατόρθωτα , είναι εφικτό να ανοιχτεί από οποιονδήποτε άλλον εκτός από τον νόμιμο παραλήπτη .

Πιστοποίηση (Authentication)

Πιστοποίηση είναι η επιβεβαίωση της ταυτότητας ενός ατόμου ή η επιβεβαίωση της πηγής αποστολής των πληροφοριών . Δηλαδή , το άτομο που επιθυμεί να επιβεβαιώσει την ταυτότητά ενός άλλου ατόμου ή κάποιου εξυπηρετητή με το οποίο επικοινωνεί , βασίζεται στην πιστοποίηση .

Η πιστοποίηση μπορεί να υλοποιηθεί με τρεις βασικές μεθόδους :

1. Κάτι που γνωρίζουμε , π.χ. το PIN μιας τραπεζικής κάρτας ή το μυστικό κωδικό ενός λογαριασμού (password) .
2. Κάτι που έχουμε στην ιδιοκτησία μας , π.χ. το κλειδί μιας πόρτας ή μια τραπεζική κάρτα .
3. Κάτι που έχουμε εκ γενετής , π.χ. δακτυλικά αποτυπώματα , φωνή κ.τ.λ.

Η Πιστοποίηση , πιο απλά , είναι ο τρόπος με τον οποίο δημοσιεύονται οι τιμές των δημόσιων κλειδιών και η πληροφορία που αντιστοιχεί στις τιμές αυτές . Ένα ***πιστοποιητικό (certificate)*** είναι ο τρόπος με τον οποίο η Υποδομή Δημοσίου Κλειδιού μεταδίδει τις τιμές των δημόσιων κλειδιών , ή η πληροφορία που σχετίζεται με αυτά , ή και τα δύο . Γενικά , ένα πιστοποιητικό είναι μία συλλογή πληροφοριών που έχει υπογραφεί ψηφιακά από την οντότητα που το εκδίδει . Τα πιστοποιητικά αυτά χαρακτηρίζονται από το είδος της πληροφορίας που περιέχουν . Η εκδότρια αρχή των πιστοποιητικών ονομάζεται ***Αρχή Πιστοποίησης (Certificate Authority – CA) .***

Ακεραιότητα (Integrity)

Ακεραιότητα είναι η προστασία των δεδομένων ενάντια σε μη εξουσιοδοτημένη τροποποίηση ή αντικατάστασή τους . Η υπηρεσία .

αυτή παρέχεται από μηχανισμούς κρυπτογραφίας όπως είναι οι ψηφιακές υπογραφές .

Ας υποθέσουμε την ακεραιότητα ενός διαφανούς φακέλου . Το μήνυμα που περιέχει ο φάκελος μπορεί να διαβαστεί από τον οποιονδήποτε , οπότε και παραβιάζεται η εμπιστευτικότητα , όπως αυτή ορίστηκε παραπάνω . Ο φάκελος θεωρείται ενδεικτικό στοιχείο παραβίασης . Ο παραλήπτης βλέποντας τον φάκελο είναι σε θέση να επιβεβαιώσει ότι ο φάκελος δεν έχει ανοιχθεί , παραβιαστεί ή ακόμη και αντικατασταθεί .

Μη Άρνηση Αποδοχής (Non – Repudiation)

Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της πιστοποίησης και της ακεραιότητας που παρέχονται σε μια Τρίτη οντότητα . Έτσι , ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί την δημιουργία και αποστολή του μηνύματος . Η ασύμμετρη κρυπτογραφία παρέχει ψηφιακές υπογραφές , τέτοιες ώστε μόνο ο αποστολέας του μηνύματος θα μπορούσε να κατέχει την συγκεκριμένη ψηφιακή υπογραφή , πρόκειται δηλαδή για μια αμφιμονοσήμαντη σχέση . Με αυτόν τον τρόπο , ο οποιοσδήποτε , και φυσικά και ο παραλήπτης του ψηφιακά υπογεγραμμένου μηνύματος μπορεί να επιβεβαιώσει την ψηφιακή υπογραφή του αποστολέα .

3.5.2 Πρότυπα Ανάπτυξης Υποδομής Δημοσίου Κλειδιού

Η Υποδομή Δημοσίου Κλειδιού υλοποιείται σύμφωνα με διεθνή πρότυπα , όπως αυτά ορίζονται από Παγκόσμιους Οργανισμούς . Όπως για παράδειγμα :

Internet Engineering Task Force , Request for Comments (IETF RFCs)

Υποδομή Δημοσίου Κλειδιού X.509 (PKIX) . Η ομάδα εργασίας PKIX (Working Group PKIX) δημιουργήθηκε το 1995 με βασικό στόχο την ανάπτυξη προτύπων Διαδικτύου (Internet Standards) αναγκαία για την υποστήριξη της Υποδομής Δημοσίου Κλειδιού . Για περισσότερες πληροφορίες μπορούμε να επισκεφτούμε τον δικτυακό τόπο http://www.ietf.org/html.charters/pkix-charter.html

Public-Key Cryptography Standards (PKCS)

Το 1991 δημοσιοποιήθηκαν οι πρώτες τεχνικές προδιαγραφές για πρότυπα Κρυπτογραφίας Δημοσίου Κλειδιού από τα εργαστήρια RSA με στόχο την επιτάχυνση της ανάπτυξης της Υποδομής Δημοσίου Κλειδιού . Οι τεχνικές αυτές προδιαγραφές αποτελούν σημείο αναφοράς για κάθε υλοποίηση Υποδομής Δημοσίου Κλειδιού , είναι γνωστές με το ακρωνύμιο PKCS και έναν συγκεκριμένο αριθμό π.χ. PKCS #1 RSA Cryptography Standard . Για περισσότερες πληροφορίες μπορούμε να επσκεφτούμε τον δικτυακό τόπο http//www.rsasecurity.com/rsalabs/pkcs/

3.5.3 Pretty Good Privacy (PGP)

Το Pretty Good Privacy ή PGP αποτελεί ένα κρυπτοσύστημα που δημιουργήθηκε από τον Phil Zimmerman και χρησιμοποιεί τους

αλγόριθμους RSA και IDEA για την κρυπτογράφηση και υπογραφή μηνυμάτων της ηλεκτρονικής αλληλογραφίας .

Κάθε χρήστης του PGP διατηρεί μια λίστα με τα δημόσια κλειδιά των χρηστών με τους οποίους επικοινωνεί , η οποία καλείται keyring . Για την προστασία της λίστας , ο κάθε χρήστης την υπογράφει με το

ιδιωτικό του κλειδί . Κάθε κλειδί που προστίθεται στην λίστα είναι δυνατό να φέρει έναν από τους εξής χαρακτήρες :

- Απολύτως Έμπιστο (Completely Trusted)
- Μερικώς Έμπιστο (Marginally Trusted)
- Μη Έμπιστο (Untrusted)
- Άγνωστο (Unknown)

Το PGP επιτρέπει την ανταλλαγή keyrings , ενώ ο κάθε χρήστης έχει την δυνατότητα να ρυθμίσει το επίπεδο εμπιστοσύνης για την αποδοχή ενός νέου κλειδιού . Δηλαδή , ο χρήστης μπορεί να θεωρήσει την οντότητα του κλειδιού έμπιστη , αν το κλειδί έχει ήδη υπογραφεί από δύο απολύτως έμπιστα (Marginally Trusted) κλειδιά .

Καθώς οι χρήστες ανταλλάσσουν keyrings σχηματίζουν έναν ιστό εμπιστοσύνης (web of trust) . Κάθε χρήστης αποτελεί αρχή πιστοποίησης του εαυτού του και είναι υπεύθυνος για το μοντέλο εμπιστοσύνης που επιλέγει . Το απλό αυτό μοντέλο έχει επιτρέψει στο PGP να κερδίσει μία σχετικά μεγάλη αποδοχή στο Διαδίκτυο . Παρόλα αυτά , η Υποδομή Δημοσίου Κλειδιού του PGP δεν είναι κατάλληλη για εφαρμογές ηλεκτρονικού εμπορίου και για εφαρμογές που απαιτούν ισχυρή ταυτοποίηση .

Τα πιστοποιητικά του PGP δεν είναι επεκτάσιμα και περιέχουν μόνο μία διεύθυνση ηλεκτρονικής αλληλογραφίας , την τιμή ενός δημόσιου κλειδιού και ένα χαρακτηριστικό του βαθμού της εμπιστοσύνης . Καθώς η διεύθυνση ηλεκτρονικής αλληλογραφίας δεν μπορεί να αποτελέσει έναν ακριβή τρόπο του προσδιορισμού της ταυτότητας ενός χρήστη , το PGP δεν μπορεί να παρέχει ισχυρή ταυτοποίηση (strong authentication) . Η έλλειψη επεκτασιμότητας των πιστοποιητικών του PGP τα καθιστά ακατάλληλα για άλλες εφαρμογές εκτός της ηλεκτρονικής αλληλογραφίας .

Το PGP δεν υποστηρίζει κάποια μέθοδο επαλήθευσης και ανάκλησης των πιστοποιητικών . Οι διαδικασίες αυτές πραγματοποιούνται μόνο μέσω άμεσης επικοινωνίας των χρηστών . Το PGP δεν παρέχει τη

δυνατότητα ανωνυμίας , καθώς η χρήση μιας διεύθυνσης ηλεκτρονικής αλληλογραφίας που δεν περιέχει κάποια ένδειξη για την ταυτότητα του χρήστη καθιστά αδύνατη την επικοινωνία μεταξύ των χρηστών για την επαλήθευση και ανάκληση των πιστοποιητικών .

3.5.4 X. 509

Το X. 509 σχεδιάστηκε για να παρέχει την υποδομή πιστοποίησης στις υπηρεσίες καταλόγου του X.500 (Idap) .Η πρώτη έκδοση του X. 509 δημοσιεύτηκε το 1988 , καθιστώντας το έτσι την παλαιότερη πρόταση για μία παγκόσμια Υποδομή Δημοσίου Κλειδιού .

Το γεγονός αυτό σε συνδυασμό με την υποστήριξη του προτύπου από τον Διεθνή Οργανισμό Τυποποίησης (International Standards Organization – ISO) και την Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunications Union – ITU) έχουν οδηγήσει στην υιοθέτηση του X .509 από μεγάλο αριθμό οργανισμών και κατασκευαστών .

Η VISA και η MASTERCARD έχουν επιλέξει το X . 509 για το Secure Electronic Transactions (SET) πρότυπο , και η NETSCAPE υιοθέτησε το X . 509 πρότυπο για την έκδοση των πιστοποιητικών που χρησιμοποιούνται στο Secure Sockets Layer πρωτόκολλο .

Η έκδοση 3 του X . 509 επεκτείνει σε μεγάλο βαθμό την λειτουργικότητα του προτύπου και γι αυτό είναι ιδιαίτερα διαδεδομένο και χρησιμοποιείται σε πλοηγητές ιστοσελίδων (web browsers) , εξυπηρετητές και προγράμματα λογισμικού για την διαχείριση του ηλεκτρονικού ταχυδρομείου (mail server / clients) κ.τ.λ. από πολλές γνωστές εταιρείες λογισμικού .

3.5.5 Ακαδημαική Εφαρμογή Υποδομής Δημοσίου Κλειδιού

Η Υποδομή Δημοσίου Κλειδιού έχει πολλές εφαρμογές σε ένα Ακαδημαικό Ίδρυμα . Όπως :

Ασφαλές Ηλεκτρονικό Ταχυδρομείο

Ο χρήστης ηλεκτρονικού ταχυδρομείου που έχει αποκτήσει προσωπικό ψηφιακό πιστοποιητικό από μια Αρχή Πιστοποίησης έχει

τη δυνατότητα να ανταλλάσσει κρυπτογραφημένα μηνύματα , διαφυλάσσοντας έτσι την ασφάλεια των μηνυμάτων του και το απαραβίαστο της προσωπικής του ηλεκτρονικής αλληλογραφίας .

Ο χρήστης κρυπτογραφεί το μήνυμα του με το δημόσιο κλειδί του παραλήπτη και το υπογράφει με την ψηφιακή του υπογραφή . Έτσι , μόνο ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα , με το ιδιωτικό του κλειδί , και να διαβάσει το περιεχόμενο του μηνύματος . Ακόμη , ο παραλήπτης είναι σίγουρος ότι ο αποστολέας είναι αυτός που δηλώνει ότι απέστειλε το μήνυμα , βασιζόμενος στην ψηφιακή υπογραφή που φέρει το μήνυμα , καθώς επίσης και ότι το περιεχόμενο του μηνύματος δεν έχει αλλοιωθεί .

Πρόσβαση σε ασφαλείς δικτυακούς τόπους

Η αποδοχή της Αρχής Πιστοποίησης συνεπάγεται την προσθήκη ψηφιακών πιστοποιητικών στον πλοηγητή (browser) του χρήστη του Διαδικτύου . Με βάση τα ιδιαίτερα χαρακτηριστικά του πιστοποιητικού αυτού , ο χρήστης έχει τη δυνατότητα να επισκεφτεί ασφαλείς δικτυακούς τόπους και να προσπελάσει δεδομένα , χωρίς αυτά να είναι δημοσιευμένα σε κοινή θέα .

Για παράδειγμα , ασφαλείς δικτυακοί τόποι είναι οι ιστοσελίδες http://mail . auth . gr και http://accounts . auth . gr για την διαχείριση του ηλεκτρονικού ταχυδρομείου και των λογαριασμών αντίστοιχα . Τα στοιχεία που υποβάλλει ο χρήστης και τα δεδομένα που βλέπει στους παραπάνω δικτυακούς τόπους δεν είναι διαθέσιμα σε κοινή θέα .

Προστασία ευαίσθητων δεδομένων σε γραμματείες τμημάτων και διοικητικούς φορείς

3. Κρυπτογράφηση

Οι γραμματείες των τμημάτων ενός Ακαδημαικού Ιδρύματος καθώς και οι διοικητικές υπηρεσίες έχουν στη διάθεσή τους ιδιαίτερα δεδομένα που πρέπει να προστατευτούν .

Η βαθμολογία των φοιτητών , τα οικονομικά στοιχεία των εργαζομένων , τα διοικητικά έγγραφα , οι πρυτανικές αποφάσεις , είναι μερικά σημαντικά δεδομένα που δεν πρέπει να είναι κοινώς προσπελάσιμα , παρά μόνο από εξουσιοδοτημένα μέλη και επίσης πρέπει να προστατεύονται από παραβιάσεις και αλλοιώσεις .

Η πιστοποίηση της ταυτότητας των χρηστών και η προστασία τέτοιου είδους δεδομένων μπορεί να επιτευχθεί με την Υποδομή Δημοσίου Κλειδιού . Με τα ψηφιακά πιστοποιητικά για τους χρήστες επιβεβαιώνεται η ασφάλεια των δεδομένων .

Προστασία ερευνητικών δεδομένων

Η προστασία ερευνητικών αποτελεσμάτων και μελετών είναι ιδιαίτερα σημαντική σε ένα ακαδημαικό ίδρυμα . Τα ευαίσθητα ερευνητικά δεδομένα που αποθηκεύονται σε εξυπηρετητές πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση . Επίσης , η δικτυακή μεταφορά τους σε εξουσιοδοτημένα μέλη της ακαδημαικής κοινότητας πρέπει να είναι ασφαλείς .

Η Υποδομή Δημοσίου Κλειδιού παρέχει μηχανισμούς ασφαλείας για αποθήκευση και μεταφορά ερευνητικών δεδομένων . Τα ερευνητικά δεδομένα κρυπτογραφούνται , έτσι ώστε μόνο εξουσιοδοτημένα μέλη να έχουν τη δυνατότητα να τα αποκρυπτογραφήσουν και να τα αποκτήσουν .

Πρόσβαση σε ηλεκτρονικές βιβλιοθήκες

Η πρόσβαση σε ηλεκτρονικές βιβλιοθήκες είναι ένα αναγκαίο εργαλείο για την ακαδημαική έρευνα και μελέτη .

Στην πλειοψηφία , οι ηλεκτρονικές βιβλιοθήκες παρέχουν τη δυνατότητα σύνδεσης χρηστών που έχουν διεύθυνση δικτύου (IP) με συγκεκριμένη μορφή (π.χ. οι χρήστες του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης μπορούν να προσπελάσουν τα ψηφιακά δεδομένα της βιβλιοθήκης του Α.Π.Θ. μόνο αν έχουν διεύθυνση δικτύου της μορφής (

155.207.x.y.) . Η λύση αυτή όχι μόνο δεν είναι ασφαλής , αλλά παρεμποδίζει και το έργο των ακαδημαικών μελών όταν αυτοί βρίσκονται εκτός του Ακαδημαικού Ιδρύματος ή συνδέονται μέσω κάποιου παροχέα δικτυακών υπηρεσιών (Internet Provider) , οπότε και αποκτούν διεύθυνση δικτύου διαφορετικής μορφής .

Τα προβλήματα αυτά μπορούν να επιλυθούν με ένα πιο ευέλικτο σχήμα ταυτοποίησης των εξουσιοδοτημένων χρηστών . Η Υποδομή

Δημοσίου Κλειδιού παρέχει ψηφιακά πιστοποιητικά για κάθε χρήστη , έτσι ώστε να επιβεβαιώνεται η ταυτότητά του και να έχει τη δυνατότητα πρόσβασης σε ηλεκτρονικές βιβλιοθήκες μόνο με βάση την ακαδημαική του ιδιότητα .

Πλέγμα Δεδομένων (Data GRID)

Το Πλέγμα Δεδομένων είναι μια σχετικά νέα έννοια στην ψηφιακή κοινωνία και αποδεικνύεται μια πολύ ουσιώδης δομή για τα Ακαδημαικά Ιδρύματα . Η δικτυακή αυτή δομή επιτρέπει σε ερευνητές , εργαστήρια και πανεπιστήμια από όλο τον κόσμο να συνενώνουν τις δυνάμεις τους για να έχουν μια δυναμική συνεργασία σε διάφορες ερευνητικές περιοχές .

Βασιζόμενοι σε μια κατανεμημένη δομή που περιλαμβάνει ηλεκτρονικές βιβλιοθήκες , δικτυακούς πόρους , χώρους αποθήκευσης ψηφιακών δεδομένων , υπολογιστικά συστήματα μεγάλης ισχύος ανά τον κόσμο , τα ακαδημαικά μέλη έχουν το δικαίωμα να χρησιμοποιήσουν τα μέσα αυτά , ανεξάρτητα από την φυσική τους τοποθεσία , με στόχο την έρευνα .

Για παράδειγμα χιλιάδες αστρονόμοι που ανήκουν σε διάφορα ακαδημαικά εργαστήρια του κόσμου και εστιάζουν σε μια ερευνητική περιοχή μπορούν να δημιουργήσουν ένα Πλέγμα Δεδομένων και να διαμοιράζονται όλα τα φυσικά μέσα που χρειάζονται για την έρευνά τους , ανεξάρτητα από την χωροταξική τους θέση .

Η πρόσβαση σε ερευνητικά δεδομένα , σε αποτελέσματα μελετών , σε δικτυακούς πόρους , σε χώρους αποθήκευσης δεδομένων και γενικότερα σε μέσα που χρησιμοποιούνται για έρευνα πρέπει να περιορίζεται μόνο σε εξουσιοδοτημένα μέλη της ακαδημαικής κοινότητας . Αυτό επιτυγχάνεται με την Υποδομή Δημοσίου Κλειδιού και με την

αντιστοίχηση ψηφιακών πιστοποιητικών σε κάθε χρήστη , ώστε να επιβεβαιώνεται η ταυτότητά τους .

Δημιουργία ερευνητικών ιστοσελίδων με δημόσια και ιδιωτικά τμήματα

Πολλά ερευνητικά προγράμματα που εκπονούνται στα πλαίσια ακαδημαικών προγραμμάτων έχουν οργανωμένες ιστοσελίδες , όπου και δημοσιεύονται διάφορα στοιχεία και αποτελέσματα για το ερευνητικό έργο που επιτελείται .

Στα ερευνητικά αυτά έργα είναι πιθανό να συμμετέχουν επιστημονικοί συνεργάτες από άλλα ακαδημαικά ιδρύματα και να κρίνεται αναγκαία η απομακρυσμένη προσπέλαση συγκεκριμένων συνεργατών στα ερευνητικά δεδομένα . Έτσι δημιουργείται η ανάγκη να υπάρχουν ιστοσελίδες που να παρέχουν πληροφορίες και να παρουσιάζουν το ερευνητικό έργο σε κάθε ενδιαφερόμενο , αλλά παράλληλα να υπάρχει η δυνατότητα απομακρυσμένης πρόσβασης από συγκεκριμένα ακαδημαικά μέλη σε δεδομένα της έρευνας που δεν είναι προς κοινή δημοσίευση .

Η διάκριση των εξουσιοδοτημένων ακαδημαικών μελών που μπορούν να έχουν πρόσβαση σε όλα τα ερευνητικά δεδομένα και στους υπόλοιπους ενδιαφερόμενους που έχουν περιορισμένη πρόσβαση , μπορεί να υλοποιηθεί με βάση την Υποδομή Δημοσίου Κλειδιού και την χρήση πιστοποιητικών . Ανάλογα με τα χαρακτηριστικά του πιστοποιητικού του χρήστη θα επιτρέπεται η αντίστοιχη προσπέλαση στην ερευνητική ιστοσελίδα .

Υποβολή Ψηφιακά Υπογεγραμμένων Εργασιών

Σε μερικά μαθήματα δίνεται η δυνατότητα υλοποίησης ή παράδοσης εργασιών μέσα από το περιβάλλον μιας ιστοσελίδας .

Η Υποδομή Δημοσίου Κλειδιού παρέχει έναν ασφαλή τρόπο να καθοριστεί ο αποστολέας της εργασίας , ότι η εργασία δεν έχει αλλοιωθεί και έχει υποβληθεί στο χρονικό διάστημα της ανάθεσης , όπως αυτό έχει αρχικά οριστεί (χρονοσφράγιση – timestaimp) .

Υπογεγραμμένο Λογισμικό

Η Υποδομή Δημοσίου Κλειδιού παρέχει ψηφιακά πιστοποιητικά σε χρήστες για να υπογράψουν το λογισμικό που αναπτύσσουν .

Οι ψηφιακές υπογραφές που συνοδεύουν το λογισμικό είναι τέτοιες ώστε οι αποδέκτες του λογισμικού να γνωρίζουν ποιος ανέπτυξε το λογισμικό καθώς επίσης και να είναι βέβαιοι ότι μπορούν να χρησιμοποιήσουν άμεσα το λογισμικό χωρίς να παρουσιαστούν προβλήματα ασφαλείας (εγκατάσταση ηλεκτρονικών ιών) .

3.5.6 Αλγόριθμοι Κρυπτογράφησης Δεδομένων

Η ασφάλεια δεδομένων αποτελεί σήμερα ένα από τα σημαντικότερα προβλήματα , που οι επιστήμονες της πληροφορικής πρέπει να αντιμετωπίσουν . Προσπάθειες προς αυτή την κατεύθυνση έχουν γίνει άλλες φορές με επιτυχία και άλλες χωρίς . Εδώ , θα παρουσιαστούν τρεις αλγόριθμοι , που αποτέλεσαν κάποιες πρώτες προσπάθειες για την κρυπτογράφηση δεδομένων . Αυτοί είναι οι :

a) Αλγόριθμος του Καίσαρα (Caesar cipher)
b) Αλγόριθμος με κλειδί πίνακα
c) Αλγόριθμος Vigenere (Vigenere cipher)

Ας δούμε λοιπόν πώς υλοποιείται κάθε αλγόριθμος :

1. Κρυπτογράφηση με τον αλγόριθμο του Καίσαρα

3. Κρυπτογράφηση

Από τις παλιότερες μεθόδους κρυπτογράφησης είναι ο αλγόριθμος του Καίσαρα , όπου αν ένα γράμμα στο αρχικό κείμενο είναι το *Νιοστό* στο αλφάβητο , αντικαθίσταται από το (N+K)ιοστό γράμμα του αλφαβήτου , όπου K είναι ένας σταθερός ακέραιος (για τον αλγόριθμο του Καίσαρα K=3) .

A. Εισάγουμε το όνομα του αρχείου που θα επεξεργαστούμε καθώς και του αρχείου αποθήκευσης ή το κείμενο προς κρυπτογράφηση , αν η είσοδος γίνεται από το πληκτρολόγιο .

B. Διαβάζουμε έναν χαρακτήρα είτε από το αρχείο είτε από το αποθηκευμένο κείμενο που δώσαμε με το πληκτρολόγιο .

C. Ελέγχουμε αν ο χαρακτήρας είναι ο χαρακτήρας αλλαγής γραμμής . Αν ναι , τότε γράφουμε στο αρχείο τον ίδιο χαρακτήρα χωρίς αλλαγή . Αλλιώς πάμε στο βήμα D .

D. Ελέγχουμε αν ο χαρακτήρας είναι το κενό . Αν είναι εμφανίζουμε το κενό στην οθόνη και γράφουμε το κενό στο αρχείο εξόδου . Αλλιώς γράφουμε στο αρχείο και στην οθόνη τον κωδικοποιημένο χαρακτήρα (χαρακτήρας + (KEY = 3)) .

E. Αν βρούμε το τέλος του αρχείου ή το χαρακτήρα τέλους των αλφαριθμητικών '\ 0 ' (αν η εισαγωγή του κειμένου γίνεται από το πληκτρολόγιο) σταματάμε . Αλλιώς πάμε στο βήμα B .

<u>Παράδειγμα χρήσης του αλγορίθμου Caesar</u>

Έστω ότι θέλουμε να κωδικοποιήσουμε το μήνυμα :
Meet me at the park

Με τον αλγόριθμο του Caesar θα γίνει :
Phhw ph dw wkh sdun

Γενικά , πάμε 3 νούμερα μπροστά από τον ASCII αριθμό του γράμματος και εμφανίζουμε το χαρακτήρα που βρίσκεται εκεί .

Αυτή η μέθοδος δεν είναι τόσο καλή , καθώς ο αναλυτής πρέπει μόνο να μαντέψει την τιμή του K : δοκιμάζοντας κάθε μια από τις 26 επιλογές , είναι σίγουρος ότι θα μπορέσει να διαβάσει το μήνυμα .

2. Κρυπτογράφηση με κλειδί πίνακα

Μια πολύ καλύτερη μέθοδος είναι να χρησιμοποιήσουμε ένα γενικό πίνακα θα ορίζει την αλλαγή που πρέπει να γίνει : για κάθε γράμμα του κειμένου προς κρυπτογράφηση , ο πίνακας λέει ποιο γράμμα να βάλουμε στο κρυπτογραφημένο κείμενο . Ο πίνακας που θα δίνει τις δικές μας αντιστοιχίες είναι ο παρακάτω (key _ arr) :

letters = [a b c d e f g h I j k l m n o p q r s t u v w x y z ! . , ?]

key _ arr = [k o a p l n j b m e u f s q c t z w d y r i v h x g ? ! * ,]

Η υλοποίηση του αλγορίθμου είναι η ακόλουθη :

A. Εισάγουμε το όνομα του αρχείου που θα επεξεργαστούμε καθώς και του αρχείου αποθήκευσης ή το κείμενο προς κρυπτογράφηση , αν η έξοδος γίνεται στην οθόνη .
B. Διαβάζουμε έναν χαρακτήρα από το αρχείο εισόδου ή από το κείμενο που δώσαμε από το πληκτρολόγιο .
C. Αναζητούμε σειριακά το χαρακτήρα στον πίνακα letters .Αν βρεθεί , γράφουμε στο αρχείο ή στην οθόνη το κωδικοποιημένο γράμμα που βρίσκεται στην αντίστοιχη θέση του πίνακα key_arr . Αλλιώς πάμε στο βήμα D .
D. Ελέγχουμε αν ο χαρακτήρας είναι η αλλαγή γραμμής , το κενό ή αν είναι αριθμός και αντίστοιχα γράφουμε στο αρχείο εξόδου ή στην οθόνη την αλλαγή γραμμής , το κενό και αν είναι αριθμός τον γράφουμε αυξημένο κατά τρία .
E. Αν έχουμε φτάσει στο τέλος του αρχείου ή αν βρήκαμε το χαρακτήρα τέλους των αλφαριθμητικών '\ 0 ' , σταματάμε . Αλλιώς πάμε στο βήμα B .

Παράδειγμα για τον αλγόριθμο με κλειδί πίνακα

Ας δούμε πώς θα γίνει το μήνυμα που χρησιμοποιήσαμε στον αλγόριθμο του Καίσαρα με τον αλγόριθμο αυτό.

Meet me at the park

Το κωδικοποιημένο μήνυμα θα είναι :

Slly sl ky ybl tkwu

Αφού το m βρίσκεται στη 13η θέση του πίνακα letters θα αντικατασταθεί με το s που βρίσκεται στην 13η θέση του πίνακα key _ arr . Ανάλογα θα αντικατασταθούν και τα υπόλοιπα γράμματα .

Αυτή είναι μια πολύ ισχυρή μέθοδος από τη μέθοδο του Καίσαρα , καθώς ο κρυπταναλυτής θα πρέπει να δοκιμάσει πολλούς περισσότερους πίνακες (περίπου 27 ! > 10*10*10.....) για να είναι σίγουρος ότι θα διαβάσει το μήνυμα . Πάντως , αλγόριθμοι « απλής αντικατάστασης » , όπως αυτός , είναι εύκολο να σπάσουν λόγω της συχνότητας εμφάνισης γραμμάτων της γλώσσας . Για παράδειγμα , αφού το Ε είναι το πιο συχνό γράμμα σε αγγλικά κείμενα , ο κρυπταναλυτής μπορεί να κάνει μια καλή αρχή στο να διαβάσει το μήνυμα με το να ψάχνει για το γράμμα που εμφανίζεται συχνότερα στο κωδικοποιημένο κείμενο και να το αντικαθιστεί με το Ε . Αν και αυτή μπορεί να μην είναι η σωστή επιλογή , είναι σαφώς καλύτερο από το να δοκιμάζεις και τα 26 γράμματα στην τύχη .

Ένας τρόπος για να κάνεις αυτό τον τύπο της επίθεσης πιο δύσκολο είναι να χρησιμοποιήσεις περισσότερους από έναν πίνακες . Ένα παράδειγμα αυτού του τύπου είναι ο αλγόριθμος Vigenere .

3. Αλγόριθμος κρυπτογράφησης Vigenere

Στον αλγόριθμο αυτό χρησιμοποιείται ένα μικρό επαναλαμβανόμενο κλειδί για να καθορίσει την τιμή του Κ για κάθε γράμμα . Σε κάθε βήμα , το γράμμα κλειδί προστίθεται στο γράμμα του κειμένου ώστε να μας δώσουν το κωδικοποιημένο γράμμα . Το κλειδί που χρησιμοποιήσαμε στον αλγόριθμό μας για την κρυπτογράφηση είναι :

Key _ table = [84 , 72 , 65 , 78 , 79 , 83] = ['T' , 'H' , 'A' , 'N' , 'O' , 'S']

Τα βήματα για την υλοποίηση του αλγορίθμου είναι τα ακόλουθα :

- Εισάγουμε το όνομα του αρχείου που θα επεξεργαστούμε καθώς και του αρχείου αποθήκευσης ή το κείμενο προς κρυπτογράφηση , αν η έξοδος γίνεται στην οθόνη και αρχικοποιούμε το μετρητή I = 0 .

- Διαβάζουμε έναν χαρακτήρα ch είτε από το αρχείο είτε από το αποθηκευμένο κείμενο που δώσαμε με το πληκτρολόγιο .

- Προσθέτουμε στον χαρακτήρα ch που διαβάσαμε τον αντίστοιχο αριθμό που βρίσκεται στη θέση key _ table[i] και παίρνουμε έτσι το κωδικοποιημένο γράμμα , το οποίο είτε γράφουμε στο αρχείο εξόδου είτε εμφανίζουμε στην οθόνη .
- Αυξάνουμε το μετρητή I κατά ένα . Αν ο μετρητής είναι ίσος με 6 τον μηδενίζουμε , αφού θέλουμε να επαναλαμβάνεται το κλειδί .
- Αν έχουμε φτάσει στο τέλος του αρχείου ή αν βρήκαμε το χαρακτήρα τέλους των αλφαριθμητικών '\0' , σταματάμε . Αλλιώς πάμε στο βήμα 2 .

<u>Παράδειγμα για τον αλγόριθμο Vigenere</u>

Ας δούμε πώς κωδικοποιείται το μήνυμα :

Meet me at the park

Με τον αλγόριθμο Vigenere :

A - | BoiHhABoHO-Aύεώ

Στον αριθμό ASCII κάθε γράμματος προστίθεται ο αριθμός της θέσης του πίνακα – κλειδιού που τους αντιστοιχεί και το αποτέλεσμα είναι ένας νέος αριθμός ASCII που δείχνει ποιος χαρακτήρας θα εμφανιστεί . Έτσι , το m έχει ASCII 109 και του αντιστοιχεί η πρώτη θέση του πίνακα key – table , δηλαδή το 84 . Επομένως , το κωδικοποιημένο γράμμα είναι ο αριθμός ASCII 193 . Ανάλογα κωδικοποιείται και το υπόλοιπο μήνυμα .

Βέβαια , δεν αρκεί μόνο να μπορείς να κρυπτογραφείς ένα κείμενο , χρειάζεται να μπορείς να το επαναφέρεις στην αρχική του μορφή ώστε να

μπορεί να διαβαστεί από το δέκτη . Διαφορετικά , δε θα μπορέσουμε να επικοινωνήσουμε σωστά και η κωδικοποιημένη πληροφορία θα χαθεί .

PUBLIC – KEY CRYPTOGRAPHY

Μέχρι πρόσφατα , οι άνθρωποι χρησιμοποιούσαν μια μέθοδο που ονομαζόταν symmetric key cryptography για να ασφαλίζουν τις πληροφορίες που μεταφέρονται μέσα σε ένα δίκτυο . Η μέθοδος αυτή ενέπλεκε ένα κλειδί , το οποίο έπρεπε να γνωρίζουν τόσο ο αποστολέας όσο και ο παραλήπτης για την κωδικοποίηση/αποκωδικοποίηση των μηνυμάτων . Το πρόβλημα ήταν ότι ακόμα και το κλειδί αυτό θα περνούσε μέσα από το δίκτυο , οπότε ήταν πιθανό να κλαπεί .

Με την μέθοδο public – key cryptography , διαφορετικά κλειδιά χρησιμοποιούνται για την κρυπτογράφηση και την αποκρυπτογράφηση , οπότε μόνο το μήνυμα πρέπει να περάσει μέσα από το δίκτυο . Κάθε σύνδεση έχει ένα ζευγάρι κλειδιών όπου το ένα κωδικοποιεί και το άλλο αποκωδικοποιεί τις πληροφορίες . Το ένα από αυτά τα κλειδιά είναι γνωστό , το άλλο όμως παραμένει προσωπικό . Έτσι , αν γίνεται μία συνδιαλλαγή με μία τράπεζα χρησιμοποιώντας το προσωπικό κλειδί , η τράπεζα βλέπει το μήνυμα και το αποκωδικοποιεί με το γνωστό κλειδί που αντιστοιχεί στο προσωπικό . Η μέθοδος αυτή είναι γνωστή και σαν ψηφιακή υπογραφή .

Εφαρμογές της κρυπτογράφησης

1.Ασφαλής προσπέλαση

Η σύνδεση ενός χρήστη σε ένα δίκτυο υπολογιστών επιτυγχάνεται με την τεχνική των συνθηματικών(passwords). Είναι γνωστό ότι η τεχνική αυτή δεν είναι ασφαλής και παρουσιάζει πλήθος προβλημάτων. Για παράδειγμα το συνθηματικό μπορεί να αποκαλυφθεί κατά την πληκτρολόγησή του σε ένα παρευρισκόμενο. Ακόμη η σύνδεση σε ένα απομακρυσμένο υπολογιστή εκθέτει το χρήστη σε υποκλοπές του συνθηματικού. Επειδή η επιλογή των συνθηματικών είναι συνήθως περιορισμένη η εύρεση τους από τρίτους μπορεί να επιτευχθεί εύκολα χωρίς ιδιαίτερη παραβίαση του συστήματος.
Μία ασφαλής προσπέλαση μπορεί να επιτευχθεί με την χρήση κρυπτογραφικών τεχνικών. Μια τέτοια τεχνική βασίζεται σε μια διαδικασία κλήσης-απόκρισης των εμπλεκομένων μερών και χρησιμοποιεί ψηφιακές υπογραφές. Σε αυτήν ο χρήστης υπογράφει μια τυχαία συμβολοσειρά του συστήματος η οποία επαληθεύεται από το σύστημα. Μια άλλη τεχνική βασίζεται σε συστήματα μηδενικής γνώσης. Σε αυτήν ο χρήστης εφοδιάζεται με μία υπογραφή της ταυτότητας του από ένα αρμόδιο κέντρο. Κατά την πραγματοποίηση μιας προσπέλασης χρησιμοποιεί ένα σύστημα μηδενικής γνώσης για να αποδείξει ότι γνωρίζει την υπογραφή χωρίς να την αποκαλύψει. Η υλοποίηση και των δύο αυτών τεχνικών μπορεί να γίνει με την χρήση έξυπνων καρτών. Μια έξυπνη κάρτα είναι μια βελτιωμένη έκδοση της συμβατικής πιστωτικής κάρτας, η οποία περιέχει έναν μικροεπεξεργαστή με συνδέσεις εισόδου-εξόδου. Ο μικροεπεξεργαστής αυτός διαθέτει περιορισμένη ασφαλή μνήμη για την καταχώρηση του μυστικού κλειδιού και άλλων στοιχείων, και μπορεί να εκτελεί βασικές πράξεις συμπεριλαμβανομένων και κρυπτογραφικών αλγόριθμων.

2.Ψηφιακά διαβατήρια

Τα διαβατήρια είναι ένας τρόπος αναγνώρισης ταυτότητας. Με την χρήση των ηλεκτρονικών υπογραφών είναι δυνατό να δημιουργηθούν ασφαλή ψηφιακά διαβατήρια. Η τεχνική είναι ανάλογη με αυτή της ασφαλούς προσπέλασης. Κάθε κράτος εκδίδει ένα ψηφιακό διαβατήριο το οποίο περιλαμβάνει μια υπογραφή της ταυτότητας του χρήστη. Έτσι, όταν ο κάτοχος του διαβατηρίου θέλει να ταυτοποιηθεί αποδεικνύει χρησιμοποιώντας ένα πρωτόκολλο μηδενικής γνώσης, ότι γνωρίζει την υπογραφή χωρίς να την επιδείξει. Επειδή η αποκάλυψη της αποδείξεως μπορεί να οδηγήσει σε πλαστογράφηση είναι απαραίτητο το ψηφιακό

διαβατήριο να υλοποιηθεί με tamper-free συσκευές όπως οι έξυπνες κάρτες.

3.Ηλεκτρονική μεταβίβαση δεδομένων

Η ηλεκτρονική μεταβίβαση δεδομένων είναι μια τεχνική ηλεκτρονικής μεταφοράς μηνυμάτων μεταξύ πληροφοριακών συστημάτων σύμφωνα με καθορισμένα πρότυπα δόμησης. Στις αναπτυγμένες εμπορικά χώρες η τεχνική αυτή αποτελεί καθημερινή πρακτική στο εμπόριο και την βιομηχανία για τη διεκπεραίωση συναλλαγών, αποφεύγοντας το συμβατικό τρόπο επεξεργασίας και ανταλλαγής εγγράφων. Σύμφωνα με αυτή, οι ανταλλασόμενες εντολές μορφοποιούνται με αυστηρά καθορισμένα πρότυπα έτσι ώστε να αναγνωρίζονται από τα υπολογιστικά συστήματα των εμπλεκομένων μερών. Η όλη διαδικασία ολοκληρώνεται εντός ελαχίστου χρόνου ηλεκτρονικά με συνέπεια να επιτυγχάνεται ο εμπορικός κύκλος

3.6 Κρυπτογράφηση-Παρελθόν και μέλλον

Η κρυπτογραφία έχει μια μεγάλη και συναρπαστική ιστορία. Η πιο πολύπλοκη όχι τεχνική εξήγηση του θέματος είναι το βιβλίο 'Kahn's The Codebreakers'. Αυτό το βιβλίο ακολουθεί τα ίχνη της κρυπτογραφίας από την αρχική και περιορισμένη χρήση της από τους Αιγυπτίους 4000 χρόνια πριν, μέχρι τον εικοστό αιώνα όπου έπαιξε ένάν αποφασιστικό ρόλο στην έκβαση και των δύο παγκόσμιων πολέμων. Ολοκληρώνοντας το 1963, το βιβλίο 'Kahn's The Codebreakers' καλύπτει αυτές τις όψεις της ιστορίας οι οποίες ήταν πολύ σημαντικές στην εξέλιξη του θέματος. Οι επικρατέστεροι κατέχοντες αυτήν την τέχνη ήταν αυτοί που συνεργάζονταν με τον στρατό, με την διπλωματική υπηρεσία και την κυβέρνηση γενικότερα. Η κρυπτογραφία χρησιμοποιήθηκε ως εργαλείο για την προστασία των εθνικών μυστικών και στρατηγικών.

Η εξάπλωση των υπολογιστών και των συστημάτων επικοινωνίας στην δεκαετία του 60 έφερε μια απαίτηση από τον ιδιωτικό τομέα να προστατευτεί η πληροφορία σε ψηφιακή μορφή και να διασφαλιστούν οι υπηρεσίες ασφαλείας. Ξεκινώντας με την εργασία του Feistel στην IBM στις αρχές της δεκαετίας του 70 και φτάνοντας στο αποκορύφωμα το 1977 με την ψήφιση ως επιπέδου επεξεργασίας αμερικάνικων ομοσπονδιακών πληροφοριών για απόκρυψη απόρρητων πληροφοριών, η DES(Data Encryption Standard) είναι ο πιο ευρέως γνωστός κρυπτογραφικός μηχανισμός στην ιστορία. Παραμένει ως ένα εχέγγυο ασφάλειας ηλεκτρονικών συναλλαγών για πολλά οικονομικά ινστιτούτα σε όλο τον κόσμο.

Η πιο εντυπωσιακή εξέλιξη στην ιστορία της κρυπτογραφίας έγινε το 1976 όταν οι Diffie και Hellman εκδώσανε τις 'New Directions in Cryptography. Αυτή η επιστημονική δημοσίευση παρουσίασε την επαναστατική ιδέα της κρυπτογράφησης δημοσίου κλειδιού και επίσης έδωσε μια νέα και έξυπνη μέθοδο για ανταλλαγή κλειδιού, την ασφάλεια της οποίας είναι βασισμένη στον δογματισμό του ξεχωριστού λογαριθμικού προβλήματος. Παρόλο που οι αρχές δεν είχαν πρακτική αντίληψη για την ιδέα απόκρυψης δημοσίου κλειδιού για την ώρα, η ιδέα ήταν ξεκάθαρη και δημιουργούσε εκτεταμένα ενδιαφέροντα και δραστηριότητες στην κοινωνία της κρυπτογραφίας. Το 1978 οι Rivest, Shamir, και Adleman ανακάλυψαν το πρώτο πρακτικό σχέδιο απόκρυψης δημοσίου κλειδιού και ταυτότητας, το οποίο τώρα αναφέρεται ως RSA. Το σχέδιο RSA είναι βασισμένο σε ένα άλλο δύσκολο μαθηματικό πρόβλημα, τον δογματισμό να παράγεις μεγάλους ακέραιους αριθμούς. Αυτή η εφαρμογή ενός δύσκολου μαθηματικού προβλήματος στην κρυπτογραφία αναγέννησε εφόδια στο να βρεθούν περισσότερες

αποδοτικές μέθοδοι. Η δεκαετία του 80 έδειξε σημαντικές προόδους αλλά καμία που να φωτοσκίαζε το RSA ανασφαλές σύστημα. Μια ακόμη κατηγορία δυνατών και πρακτικών μεθόδων δημοσίου κλειδιού ανακαλύφθηκε από το ElGamal το 1985. Αυτές ήταν εξίσου βασισμένες στο ξεχωριστό λογαριθμικό πρόβλημα.

Μια από τις πιο σπουδαίες συνεισφορές που παρείχε η κρυπτογράφηση δημόσιου κλειδιού είναι η ψηφιακή υπογραφή. Το 1991 θεσπίστηκε το πρώτο διεθνές πρότυπο για ψηφιακές υπογραφές. Ήταν βασισμένο στο σχέδιο δημόσιου κλειδιού του RSA. Το 1994 η κυβέρνηση των Ηνωμένων Πολιτειών θέσπισε το πρότυπο ψηφιακής υπογραφής, έναν μηχανισμό βασισμένο στη μέθοδο δημόσιου κλειδιού του ElGmal.

Η έρευνα για νέα σχέδια δημόσιου κλειδιού, βελτιώσεις σε υπάρχοντες μηχανισμούς κρυπτογράφησης, και αποδείξεις ασφάλειας συνεχίζονται με γοργά βήματα. Διάφορα πρότυπα και υποδομές που περιλαμβάνουν κρυπτογραφία τακτοποιούνται. Προϊόντα ασφαλείας βελτιώνονται για να διεκπεραιώσουν τις ανάγκες ασφάλειας μιας κοινωνίας διεξοδικών πληροφοριών.

Η κρυπτογράφηση, μέσω των χρόνων, υπήρξε μια τέχνη που πραγματοποιήθηκε από πολλούς που εφάρμοσαν τεχνικές για να συναντήσουν κάποιες από τις απαιτήσεις ασφάλειας πληροφοριών. Τα τελευταία είκοσι χρόνια υπήρξε μια περίοδος μετάβασης καθώς η πειθαρχία άλλαξε από μια τέχνη σε επιστήμη. Υπάρχουν τώρα μερικά διεθνή επιστημονικά συμβούλια αφιερωμένα αποκλειστικά στην κρυπτογραφία και επίσης ένας διεθνής επιστημονικός οργανισμός, the International Association for Cryptography Research(IACR), που έχει σκοπό την διεξοδική έρευνα σε όλο τον κόσμο.

Άλλοι πιθανοί τρόποι διασφάλισης

Με τον όρο κακόβουλη επίθεση(malicious attack), εννοούμε την κακόβουλη προσπάθεια για προσβολή ενός συστήματος πληροφοριών και της λειτουργικότητας του μέσω μιας σειράς μη επιτρεπτών, ύπουλων και κακής πρόθεσης δραστηριοτήτων. Οι δραστηριότητες αυτές κατατάσσονται σε δύο πλατιές κατηγορίες. Είναι η κατηγορία των ιών(viruses) και η κατηγορία των παρεισφρήσεων(intrusions).

Η αντιμετώπιση των κακόβουλων επιθέσεων γίνεται με δύο βασικούς τρόπους. Είτε με διαδικασίες ανίχνευσης τους και άμεσης λήψης μέτρων αντιμετώπισης τους, ή με διαδικασίες πρόβλεψης και προστασίας των συστημάτων μέσω προληπτικής επέμβασης. Έτσι έχουμε δύο μεγάλες κατηγοριοποιήσεις ανίχνευσης, την ανίχνευση δια της παρουσίας και την ανίχνευση δια της συμπεριφοράς.

Αρκετοί μηχανισμοί έχουν υλοποιηθεί υιοθετώντας την προσέγγιση της ανίχνευσης δια της παρουσίας. Τέτοιοι είναι οι σαρωτές αρχείων και ελεγκτές ακεραιότητας, αλλά και μηχανισμοί προστασίας μέσω λογισμικού για αυτοάμυνα, αλλαγής ελέγχου και ανοχής σφάλματος. Το χαρακτηριστικό αυτών των μηχανισμών είναι ότι ανιχνεύουν την επίθεση ανιχνεύοντας την παρουσία του επιτιθέμενου ή την παρουσία κάποιου αποτελέσματος της επίθεσης.

Τεχνικές τεχνητής νοημοσύνης χρησιμοποιούνται σχεδόν αποκλειστικά για την ανίχνευση δια της συμπεριφοράς. Τρεις είναι οι βασικές εφαρμόσιμες μορφές μέσω των οποίων επιχειρείται η ανίχνευση δια της συμπεριφοράς:1) Τα έμπειρα συστήματα, 2) τα συστήματα νευρωνικών δικτύων και 3) τα συστήματα που βασίζονται σε μοντέλα χρήσης.

Τα έμπειρα συστήματα είναι τις περισσότερες φορές τα πιο συνηθισμένα αυτής της κατηγορίας. Η βασική φιλοσοφία τους έγκειται στο πρόβλημα ελέγχου επιτρεπτότητας με βάση τρεις θεμελιώδεις οντότητες καθορισμού επιτρεπτότητας πρόσβασης, τα υποκείμενα, τα αντικείμενα και τα δικαιώματα πρόσβασης.

Η βάση της χρήσης των νευρωνικών δικτύων έγκειται στα εξής τρία χαρακτηριστικά: Προσαρμοστικότητα, δηλαδή ικανότητα να αναδιοργανώνουν δυναμικά, γενικευσιμότητα, δηλαδή ικανότητα να μπορούν να αποδώσουν ικανοποιητικά σε όχι καλά ορισμένες περιπτώσεις ή σε καταστάσεις θορύβου και τέλος ικανοποιητική αντιμετώπιση χρονικά εξελισσόμενων καταστάσεων.

Το κύριο χαρακτηριστικό των συστημάτων που χρησιμοποιούν μοντέλα χρήσης είναι η συνολικότερη γνώση για την χρήση του συστήματος. Αυτή η συνολικότερη γνώση είναι οργανωμένη σε μεγάλες οντότητες, τα καθήκοντα(tasks) και οι συγκρίσεις που πραγματοποιούνται δεν είναι μόνο στο επίπεδο των θεμελιωδών πράξεων οι οποίες σχηματίζουν ένα καθήκον/εργασία, αλλά συνολικά σε ολόκληρο το καθήκον/εργασία.

Ανιχνευτές ιών

Οι ανιχνευτές ιών(file scanners) είναι προϊόντα λογισμικού τα οποία ανιχνεύουν έναν ιό με βάση την ύπαρξη ή όχι της ψηφιακής τους ταυτότητας σε ένα εκτελέσιμο αρχείο. Για να εκτελεσθεί αυτή η διαδικασία, το λογισμικό πρέπει να χρησιμοποιήσει ένα αρχείο που περιέχει τις ψηφιακές ταυτότητες των γνωστών προγραμμάτων ιών. Συμπερασματικά οι ανιχνευτές ιών: Έχουν μικρό κόστος και η εφαρμογή τους απαιτεί σχετικά περιορισμένο χρόνο. Χρησιμοποιούνται με απλό τρόπο. Είναι προσανατολισμένοι σε μια κατηγορία λειτουργικών συστημάτων(κυρίως DOS). Η αξιοπιστία τους εξαρτάται από το αρχείο των ψηφιακών ταυτοτήτων. Δεν μπορούν να ανιχνεύσουν ιούς χωρίς ψηφιακή ταυτότητα ή νέους ιούς. Ανιχνεύουν την ύπαρξη της πλειοψηφίας των γνωστών ιών.
Συνεπώς οι ανιχνευτές ιών αποτελούν ένα αποδοτικό μέσο σε περιβάλλοντα με μη υψηλές απαιτήσεις ασφαλείας ή όπου οι διαθέσιμοι πόροι για την προστασία του είναι περιορισμένοι.

Αντίδοτα

Τα αντίδοτα(vaccines) είναι προϊόντα λογισμικού σχεδιασμένα για την ανίχνευση και απομάκρυνση συγκεκριμένων ιών. Η σχεδίαση τους στηρίζεται στη διατύπωση ότι οι πολλοί διαδεδομένοι ιοί είναι περιορισμένου πλήθους και ότι απαιτείται όχι μόνον η ανίχνευση ενός ιού αλλά και η απομάκρυνση του. Η ανίχνευση των ιών γίνεται με βάση την ψηφιακή τους ταυτότητα. Η απομάκρυνσή τους γίνεται με βάση οδηγίες που έχουν προκύψει ως αποτέλεσμα της ανάλυσης του πηγαίου κώδικα των ιών αυτών. Συμπερασματικά, τα αντίδοτα:
Έχουν μικρό κόστος και η εφαρμογή τους απαιτεί περιορισμένο χρόνο. Ανιχνεύουν και απομακρύνουν ένα περιορισμένο πλήθος ευρέως διαδεδομένων ιών. Είναι προσανατολισμένοι σε μια κατηγορία λειτουργικών συστημάτων(DOS). Για να αντιμετωπίσουν μεγάλο πλήθος ιών πρέπει να ανασχεδιασθούν και αυτό απαιτεί υψηλό κόστος.
Άρα, τα αντίδοτα αποτελούν ένα αποδοτικό μέσο ανίχνευσης και απομάκρυνσης ιών σε περιβάλλοντα που θεωρείται ότι είναι ευπαθή μόνο

σε συγκεκριμένους ιούς ή σε περιβάλλοντα όπου οι διαθέσιμοι πόροι για την προστασία τους είναι περιορισμένοι.

3.7 ΤΡΟΠΟΙ ΔΙΑΣΦΑΛΙΣΗΣ

ΑΣΦΑΛΕΙΣ ΕΞΥΠΗΡΕΤΗΤΕΣ

Η εταιρεία Netscape Corporation έχει επινοήσει μία τεχνολογία γνωστή ως ' ασφαλής εξυπηρετητής' (secure server) . Χρησιμοποιεί ένα πρωτόκολλο ασφαλείας που ονομάζεται SSL (Secure Sockets Layer) , το οποίο εξασφαλίζει απόκρυψη πληροφοριών , γνησιότητα του εξυπηρετητή , ακεραιότητα του μηνύματος και γνησιότητα του πελάτη . Όταν ένας χρήστης συνδεθεί με έναν ασφαλή εξυπηρετητή , ανταλλάσσεται μία 'χειραψία' που ξεκινάει την ασφαλή διαδικασία . Με το πρωτόκολλο αυτό , ένας εξυπηρετητής μπορεί να υποστηρίζει και ασφαλείς και μη-ασφαλείς πληροφορίες . Έτσι , η εταιρεία είναι σε θέση να δίνει γενικές πληροφορίες σε όλο τον κόσμο , αλλά ταυτόχρονα να περιέχει και άλλα δεδομένα που είναι κρυφά και η πρόσβαση σε αυτά είναι ελεγχόμενη . Για παράδειγμα , ένα μαγαζί του Internet μπορεί να προσφέρει τον κατάλογο των προιόντων του χωρίς καμιά ασφάλεια , αλλά να εγγυάται την παραγγελία και την πληρωμή για τις αγορές των πελατών .

Όσο το Internet προχωράει , όλο και περισσότερες οικονομικές συναλλαγές θα γίνονται σε αυτό . Αυτή τη στιγμή οι συναλλαγές γίνονται με μετάδοση της πιστωτικής κάρτας μέσω δικτύου ή μέσω τηλεφώνου . Σε μερικά χρόνια , αναμένεται η χρήση ψηφιακών χρημάτων στο Internet . Υπάρχουν δύο βασικά είδη ψηφιακών χρημάτων , τα **anonymous cash** και τα **identified cash** . Τα anonymous cash είναι το ανάλογο των χαρτονομισμάτων που χρησιμοποιούνται σήμερα . Δεν περιέχουν καθόλου πληροφορίες για τον άνθρωπο που τα έχει και δεν αφήνει κανένα σήμα στην συναλλαγή . Δημιουργούνται μέσω αριθμημένων λογαριασμών τραπέζης και τυφλών υπογραφών . Αντιθέτως , τα identified cash περιέχουν πληροφορίες για την ταυτότητα του κατόχου . Όπως γίνεται με τις πιστωτικές κάρτες , τα identified cash μπορούν να παρακολουθούνται όταν μεταφέρονται μέσω του συστήματος και δημιουργούνται μέσω πλήρως προσδιοριζόμενων λογαριασμών τραπέζης και προσωπικών υπογραφών .

ΠΡΟΣΩΠΙΚΗ ΑΣΦΑΛΕΙΑ

Το Internet έχει εξελιχθεί σε ένα πάρα πολύ ισχυρό μέσο για επικοινωνία ή δουλειές , το οποίο όμως δεν υπόκειται σε απολύτως κανένα κανόνα όσον αφορά την λειτουργία του . Λόγω της εξάπλωσης αυτής πολλές πολιτικές και κυβερνητικές οργανώσεις θέλουν να το ελέγξουν .

Παρ'ότι μερικά στοιχεία του Internet μπορούν να ρυθμιστούν σε κάποιο βαθμό , αυτό δεν είναι ιδιαίτερα εύκολο . Η φύση του Internet , ένα χαλαρό σύνολο από εκατομμύρια υπολογιστές διάσπαρτους στη γη , το καθιστά πολύ δύσκολο έως αδύνατο να ελεγχθεί . Την ίδια στιγμή , η έλλειψη ελέγχου σημαίνει ότι η προσωπική ασφάλεια του καθενός που είναι στο δίκτυο κινδυνεύει με εισβολή από κάποιον που έχει τις απαραίτητες τεχνικές γνώσεις .

Παρότι η απειλή από τους hackers είναι χαμηλή σε προσωπικό επίπεδο , μία πιο σοβαρή απειλή έρχεται από εταιρείες που λειτουργούν web sites . Πολλά sites απαιτούν από τον χρήστη να εγγράφεται πριν χρησιμοποιήσει τις υπηρεσίες που προσφέρει . Οι πληροφορίες που ζητούνται είναι συνήθως το όνομα , η διεύθυνση , το e-mail και το επάγγελμα . Στη συνέχεια , καθώς ο χρήστης περιηγείται στην σελίδα , συλλέγονται πληροφορίες για το ποιες σελίδες επισκέφτηκε , πόσο χρόνο έμεινε στο site , ποιες συνδέσεις ακολουθήθηκαν , ποια στοιχεία αναζητήθηκαν και άλλα . Τελικά , δημιουργείται ένα προφίλ του χρήστη . Το ερώτημα είναι τι κάνουν οι διαχειριστές του site με αυτό .

Οι περισσότεροι υποστηρίζουν ότι γίνονται για να προσωπικοποιείται η επίσκεψη στα sites . Για παράδειγμα , αν ένα site που ασχολείται με παιχνίδια , 'δει' ότι η προτίμηση του χρήστη είναι τα παιχνίδια στρατηγικής , την επόμενη φορά που θα μπει στο site , θα του παρουσιάσει πληροφορίες για νέα παιχνίδια στρατηγικής που έχουν βγει στην αγορά . Όμως , μερικά sites πουλάνε τις πληροφορίες αυτές σε εμπόρους και έτσι μπορεί να δέχεται ο χρήστης συνεχώς διαφημίσεις και καταλόγους για παιχνίδια μέσω e-mail .

Για να μην συμβαίνουν τα παραπάνω , πρέπει να γίνει μία ρύθμιση στις επιλογές του browser έτσι ώστε να απορρίπτονται τα αρχεία που ονομάζονται **cookies** . Το cookie είναι ένα μικρό αρχείο το οποίο

δημιουργείται και αποθηκεύεται στον υπολογιστή του χρήστη από το site που ζητά τις πληροφορίες . Όσο ο χρήστης περιηγείται στο site , όλο και περισσότερες πληροφορίες εγγράφονται στο cookie . Έτσι την επόμενη φορά που ο χρήστης θα μπει στο site , το αρχείο αυτό θα μεταφερθεί έτσι ώστε το site να αναγνωρίσει τον χρήστη .

Το cookie μπορεί να διαβαστεί μόνο από το site που το δημιούργησε και δεν δίνει πρόσβαση σε άλλα αρχεία του υπολογιστή . Τα cookies μπορούν να φανούν χρήσιμα σε περιπτώσεις αποθήκευσης passwords , έτσι ώστε να μην είναι υποχρεωτική η απομνημόνευση του . Για να ελεγχθούν τα cookies στο Netscape Navigator , η επιλογή βρίσκεται στο μενού Preferences και μετά στις επιλογές Edit και Advanced . Εκεί είναι δυνατή η αποδοχή ή απόρριψη των cookies , όπως επίσης υπάρχει η επιλογή να ρωτάει ο χρήστης πριν την τοποθέτηση ενός cookie στον υπολογιστή του . Στον Internet Explorer , οι αντίστοιχες εντολές βρίσκονται στο μενού Options και μετά Tools και Security .

Η προσωπική ασφάλεια των χρηστών προφυλάσσεται και με την χρησιμοποίηση **απόκρυψης ,** η οποία είναι μία μορφή κρυπτογράφησης . Η απόκρυψη χρειάζεται ειδικό software για την κωδικοποίηση του e-mail του χρήστη ή άλλων αρχείων που πρέπει να σταλούν με ασφάλεια στο δίκτυο . Ο παραλήπτης των αρχείων αυτών χρειάζεται το αντίστοιχο software για την αποκωδικοποίηση τους .

ΠΕΡΙΛΗΨΗ

Η παρουσίαση των τρόπων με τους οποίους γίνεται η διασφάλιση των πληροφοριών και δεδομένων στο INTERNET, αποτελούν το σκοπό της παρακάτω πτυχιακής εργασίας.
Στην εργασία γίνεται αναφορά στις απειλές και τους κινδύνους που υπάρχουν στο διαδίκτυο. Παράλληλα αναφέρονται τρόποι αντιμετώπισης και καταπολέμησης των απειλών αυτών.
Γίνεται εκτενής περιγραφή στην επιστήμη της κρυπτογραφίας, που και πως χρησιμοποιείται. Επίσης γίνεται αναφορά σε μεθόδους κρυπτογράφησης καθώς και στον τρόπο υποδομής δημόσιου κλειδιού. Τέλος γίνεται αναφορά στους πιθανούς τρόπους διασφάλισης απέναντι στις απειλές και τους κινδύνους που «πολεμούν» κατά συχνά χρονικά διαστήματα το διαδίκτυο .

4. ΣΥΜΠΕΡΑΣΜΑ

Είναι προφανές ότι η εξέλιξη των τεχνολογιών πληροφορίας και τηλεπικοινωνιών, καθιστά ολοένα και δυσκολότερη την διασφάλιση πληροφοριών και δεδομένων στο INTERNET, καθώς η ποσότητα των δεδομένων που γίνονται αντικείμενο επεξεργασίας, ο συνολικός αριθμός των χρηστών τέτοιων δεδομένων και η ταχύτητα μεταφοράς των δεδομένων αυξάνονται ραγδαίως. Η λύση του προβλήματος αυτού βρίσκεται σε μεγάλο βαθμό στην ίδια την τεχνολογία.

Η τεχνολογία είναι αναγκασμένη να στρέψει το ενδιαφέρον της στην ανάπτυξη εκείνων των μεθόδων που θα καθιστούν ασφαλής την μεταφορά των πληροφοριών διαμέσου του διαδικτύου. Για την προστασία των δεδομένων έχουν προγραμματισθεί μελέτες τεχνολογικού χαρακτήρα στα πλαίσια του προγράμματος της Ευρωπαϊκής Ένωσης για την ασφάλεια των πληροφοριών, που έχει ως στόχο την εμπιστευτικότητα, την πληρότητα και την διαθεσιμότητα στις ηλεκτρονικές πληροφορίες. Βέβαια τα μέτρα αυτά που παίρνει η Ε.Ε. αποτελούν ένα μικρό μέρος της πιθανής συμβολής της τεχνολογίας στην αποτελεσματική προστασία των πληροφοριών και των δεδομένων.

Συνεπώς, μια αποτελεσματική πολιτική ασφάλειας και προστασίας των δεδομένων στο διαδίκτυο, και όχι μόνο, πρέπει να υλοποιηθεί με τρόπο που να εξασφαλίζει ένα αποδεκτό επίπεδο προστασίας μέσα σε ένα ηλεκτρονικό περιβάλλον λαμβάνοντας υπόψη το ανάλογο νομικό πλαίσιο και το σχετικό κώδικα δεοντολογίας. Αν δεν γίνει αυτό θα ανοίξει ο δρόμος της εξάπλωσης του ηλεκτρονικού εγκλήματος και των καταχρήσεων των πληροφοριών και των προσωπικών δεδομένων.

ΠΗΓΕΣ-ΣΧΕΤΙΚΟΙ ΣΥΝΔΕΣΜΟΙ

ΕΛΛΗΝΙΚΑ SITE

http://www.gunet.gr

http://www.mxd.gr

http://noc.auth.gr

http://www.netmode.ntua.gr

http://www.de.sch.gr

http://www.it.uom.gr

ΞΕΝΑ SITE

http://world.std.com

http://www.cryptography.com

http://www.cacr.math.unwaterloo.ca