ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ & ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Η Συμβολή της Κρυπτογραφίας στις Σύγχρονες Οικονομικές Συναλλαγέςε»

ΖΑΚΚΑ ΑΝΝΑ

ΝΙΚΟΛΑΚΗ ΕΥΑΓΓΕΛΙΑ

ΝΟΣΤΗ ΑΓΓΕΛΙΚΗ

ΕΠΟΠΤΕΥΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ: Α. ΚΑΛΑΠΟΔΗ

ΠΑΤΡΑ 2013

ΠΡΟΛΟΓΟΣ

Αποτελεί γεγονός, πως η εφαρμογή των διαφόρων συστημάτων κρυπτογραφίας από μέρους των επιχειρήσεων και των τραπεζών με σκοπό την προστασία των πελατών τους στις ηλεκτρονικές οικονομικές συναλλαγές που διεξάγουν, είναι μια ιδιαίτερα διαδεδομένη περίπτωση και στην οποία καταφεύγουν στις μέρες μας όλο και περισσότερες επιχειρήσεις.

Κάθε ένας από εκείνους οι οποίοι εργάζονται σε μια επιχείρηση ή έναν κυβερνητικό οργανισμό, μπορεί να εφαρμόσει έναν αμυντικό «πληροφοριακό πόλεμο» ή ένα σύστημα κρυπτογράφησης. Πιο συγκεκριμένα, «πρόκειται για μια άμυνα η οποία έχει ως σκοπό να προστατέψει την ανταγωνιστικότητα και πηγές πληροφοριών των επιχειρήσεων αυτών».

Σχετικά με τους κυβερνητικούς οργανισμούς, μέσω της άμυνας που προσπαθούν να αντιτάξουν εκείνοι έναντι του «πληροφοριακού πολέμου», επιθυμούν την προστασία της εθνικής ασφάλειας των πολιτών και την διατήρηση της τάξης και των νόμων.Ο σχεδιασμός του συστήματος βάσεως δεδομένων ασφαλείας για οικονομικές συναλλαγές οφείλει να αποτελεί τμήμα του αρχικού σχεδιασμού του συστήματος και όχι μια διαδικασία που θα εκτελείται μετά την εγκατάσταση του συστήματος. Οι λόγοι είναι απλοί. Αφενός είναι οικονομικότερο να σχεδιάζονται και να υλοποιούνται ταυτόχρονα το σύστημα και η ασφάλεια του και αφετέρου είναι λειτουργικότερο.

Τα κρυπτογραφικά συστήματα για εκτέλεση οικονομικών συναλλαγών τα οποία βασίζονται στις ελλειπτικές καμπύλες για τη προστασία της βάσης δεδομένων, αποτελούν ουσιαστικά ένα πολύ σημαντικό κομμάτι της κρυπτογραφίας «δημόσιου κλειδιού» και τα τελευταία χρόνια αποκτά όλο και περισσότερο ενδιαφέρον καθώς πολλοί επιστήμονες έχουν ξεκινήσει να ασχολούνται ενεργά με τη μελέτη τους. Το πλεονέκτημα των συστημάτων αυτών σε σχέση με τα συμβατικά κρυπτογραφικά συστήματα όπως τα RSA , προσφέροντας τα ίδια επίπεδα ασφάλειας. Για το λόγο αυτό, τα κρυπτογραφικά συστήματα ελλειπτικών καμπυλών προτιμούνται τις περισσότερες φορές να χρησιμοποιούνται σε συσκευές περιορισμένων πόρων, όπως οι έξυπνες κάρτες - smart cards καθώς και στα κινητά τηλέφωνα.

Ως αποτέλεσμα και προκειμένου να ολοκληρωθεί ο σκοπός της εργασίας και ο οποίος αναφέρεται παραπάνω, η πτυχιακή εργασία διαχωρίζεται σε τρία (3) αντίστοιχα κεφάλαια μέσω των οποίων παρουσιάζεται η έννοια της κρυπτογράφησης και η εξέλιξη της απο τα πρώτα χρόνια που χρησιμοποιήθηκε εως σήμερα. Ο διαχωρισμός της στα είδη της και η σχέση της κάθεμιας από αυτές στην επιχείρηση. Τέλος, παρουσιάζεται η σχέση λειτουργίας της κρυπτογραφίας με αλγόριθμους και για κάθε ένα από τα είδη της. Στο δεύτερο κεφάλαιο παρουσιάζονται οι εφαρμογές της κρυπτογραφίας στις σύγχρονες οικονομικές συναλλαγές, εκτός από τη σχέση Επιχείρηση- Κράτους και αυτή του Πολίτη- Κράτους αναφέρονται και μεμονωμένες χρήσεις της ενώ στο τέλος του κεφαλάιου γίνεται λόγος για άλλες χρήσεις της. Στο τελευταίο κεφάλαιο της πτυχιακής παρουσιάζονται οι τρόποι τους με τους οποίους οι μέθοδοι διεξαγωγής συναλλαγών θα πρέπει να εφαρμοσθούν για να αποτελέσουν σε τελική βάση μια σωστή και αποτελεσματική «ασπίδα» προστασίας για τους πολίτες και τους επιχειρηματίες μιας κοινωνίας και οι οποίοι χρησιμοποιούν σε καθημερινή βάση τις ηλεκτρονικές οικονομικές συναλλαγές.

ΕΙΣΑΓΩΓΗ

Καθώς η πληροφορία εξελίσσεται σε όλο και πιο πολύτιμο αγαθό και καθώς η επανάσταση στις επικοινωνίες αλλάζει την κοινωνία, η διαδικασία της κωδικοποίησης των μηνυμάτων γνωστή και ως κρυπτογράφηση παίζει ολοένα και περισσότερο ρόλο στην καθημερινή μας ζωή. Η επιθυμία για μυστικότητα οδήγησε τα έθνη να οργανώσουν υπηρεσίες κωδικοποίησης υπεύθυνες για τη διασφάλιση του απορρήτου επικοινωνιών με την επινόηση και εφαρμογή καλύτερων δυνατών κωδικών. Και οι δύο πλευρές στην προσπάθεια τους να διαφυλάξουν και να καταλύσουν το απόρρητο αντλούν από ένα ευρύ φάσμα επιστημών και τεχνολογιών από μαθηματικά ως γλωσσολογία και από τη θεωρία της πληροφορίας ως τη κβαντική φυσική. Σκοπός λοιπόν της κρυπτογραφίας είναι να παρέχει μηχανισμούς προκειμένου να επικοινωνήσουν δύο ή περισσότερα μέλη χωρίς την παρέμβαση κάποιου άλλου όπου θα είναι σε θέση να διαβάσει την πληροφορία.

Αναλυτικότερα, εκτός απο την επικοινωνία των εξουσιοδοτημένων χρηστών παρέχει μέσα προκειμένου η πληροφορία αυτή να μπορεί να αλλοιωθεί αλλά μόνο από αυτούς. Επιπρόσθετα, κανένας από τους εξουσιοδοτημένους χρήστες δεν μπορεί να ισχυριστεί τη μη μετάδοση ή τη μη δημιουργία της πληροφορίας. Τέλος, γίνεται εξακρίβωση της ταυτότητας των μελών προκειμένου να αποδειχθεί ότι δεν είναι πλαστές.

Ιστορικά, και με βάση τη γλωσσική υποδομή κατά κύριο λόγο, χρησιμοποιήθηκε για να μετατρέπει μια κατανοητή πληροφορία σε μια δυσνόητη όπου μπορούσε να διαβαστεί μόνο με τη βοήθεια ενός γρίφου. Χωρίς τη γνώση του η πληροφορία θα ήταν άχρηστη. Στις νεότερες μορφές της η κρυπτογραφία χρησιμοποιεί διακριτά μαθηματικά, στατιστική συνδυαστική ανάλυση και πολλές ακόμα επιστήμες προκειμένου να παρέχει ασφάλεια.

Οι προσωπικοί υπολογιστές δεν είναι σε θέση να γνωρίζουν την ταυτότητα των χρηστών τους και γι αυτό δίνεται πλήρη πρόσβαση σε οποιονδήποτε κάνει χρήση του πληκτρολογίου. Σήμερα όμως, ένας υπολογιστής μπορεί να έρθει σε επαφή με άλλα δίκτυα μεταφέροντας ευαίσθητες πληροφορίες μιας επιχείρησης. Για αυτόν τον λόγο λοιπόν είναι απαραίτητη η αναγνώριση της ταυτότητας των χρηστών ουτως ώστε να αποκτήσουν το δικαίωμα χρήσης στις υπηρεσίες του. Η χρήση ενός password ή μιας smart card είναι δύο από τους τρόπους προστασίας.

Με τη χρήση του internet και την απλοποίηση κατά ένα μέρος των συναλλαγών με τη βοήθεια του γίνεται λόγος για την ασφάλεια των οικονομικών συναλλαγών. Πιο συγκεκριμένα, σε μια προσπάθεια εξέλιξης των τραπεζικών συναλλαγών δημιουργήθηκε το ***e-Banking***. Τα πράγματα σε αυτή τη συναλλαγή θεωρούνται να είναι κάπως πιο περίπλοκα όσον αφορά την εταιρική και τη τραπεζική ευθύνη. Σαφώς υπάρχει ένας αρκετά αυστηρός έλεγχος από την ίδια την τράπεζα και σχετικά με το επίπεδο της ασφάλειας των ηλεκτρονικών τραπεζικών συναλλαγών αλλά και σε σχέση με την αντίστοιχη ηλεκτρονική χρήση των πιστωτικών καρτών από μέρους των πολιτών. Η εξέλιξη του e-banking οδήγησε αργότερα στα ηλεκτρονικά καταστήματα όπου για την πληρωμή των ειδών ή των υπηρεσιών τους απαιτούν ηλεκτρονικό χρήμα.

Παρόλα αυτά η ασφάλεια που παρέχει η κρυπτογραφία δεν παρουσιάζεται μόνο στα οικονομικά θέματα και στην χρήση των υπολογιστών. Η σταθερή τηλεφωνία μέσω cryptophones και η κινητή μέσω ΤΕΤΡΑ-ΤΕΤΡΑΠΟΛ-GSM χρησιμοποιεί κρυπτογράφηση. Επιπρόσθετα, δίκτυα όπως τα στρατιωτικά, τα διπλωματικά όπου στέλνουν τηλεγραφήματα, τα ασύρματα δίκτυα όπως Bluetooth αλλά και η επικοινωνία μέσω διαδικτύου έχουν τις βάσεις τους στην κρυπτογραφία. Τέλος, κάτι που ίσως δεν είναι γνωστό είναι πως και τα συστήματα βιομετρικής αναγνώρισης κάνουν εκτενή χρήση της.

Κεφάλαιο Πρώτο : Η Έννοια της Κρυπτογραφίας

Για αυτό το κεφάλαιο χρησιμοποιήθηκε η εξής βιβλιογραφία: [3],[4],[6],[10],[13],[16],[20],[27],[28]

Η λέξη κρυπτογραφία προέρχεται από τα συνθετικά ‘’κρύπτος + γράφω’’ και είναι ο επιστημονικός κλάδος που ασχολείται με τη μελέτη, την ανάπτυξη και τη χρήση μεθόδων προκειμένου να κρυπτογραφούνται και να αποκρυπτογραφούνται μηνύματα. Κρυπτογραφία (cryptography) είναι η μελέτη τεχνικών που βασίζονται σε μαθηματικά προβλήματα δύσκολο να λυθούν. Ο κύριος στόχος της, είναι να δώσει την δυνατότητα σε δύο πρόσωπα, έστω Α και Β, να επικοινωνήσουν μέσα από έναν μη ασφαλές χώρο ώστε ένα τρίτο και μη εξουσιοδοτημένο πρόσωπο, Γ, να μην μπορεί να αντιληφθεί το περιεχόμενο των μηνυμάτων και να παρεμβληθεί στην επικοινωνία. Η Κρυπτανάλυση (cryptanalysis) είναι η επίλυση αυτών των προβλημάτων και κρυπτολογία (cryptology) είναι ο συνδυασμός της κρυπτογραφίας και κρυπτολογίας σε ένα ενιαίο επιστημονικό κλάδο. Εφαρμογή της κρυπτογραφίας είναι η κρυπτογράφηση.Με τον όρο κρυπτογράφηση (encryption) εννοούμε τον μετασχηματισμό των δεδομένων σε μορφή που δεν μπορεί να διαβαστεί από κανένα παρά μόνο από αυτόν που διαθέτει ένα κατάλληλο κλειδί. Η αντίστροφη διαδικασία που το κρυπτογραφημένο μήνυμα έρχεται ξανά στην αρχική του μορφή ονομάζεται αποκρυπτογράφηση (decryption).

1. Ιστορική Αναδρομή στη Κρυπτογραφία

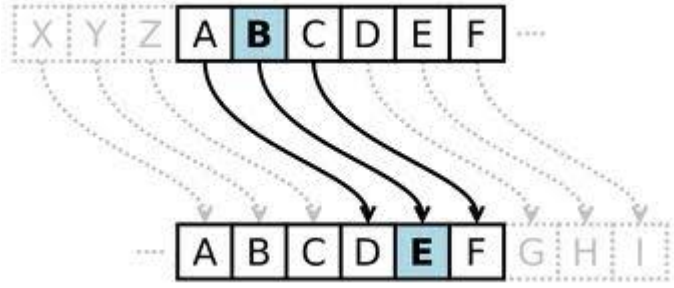
1.1 Ιστορική Αναδρομή στη Κρυπτογραφία

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για την κρυπτογράφηση μηνυμάτων δηλαδή μετατροπή της πληροφορίας από μια κανονική κατανοητή μορφή σε έναν γρίφο, που χωρίς την γνώση του κρυφού μετασχηματισμού θα παρέμενε

ακατανόητος. Κύριο χαρακτηριστικό των παλαιότερων μορφών κρυπτογράφησης ήταν ότι η επεξεργασία γινόταν πάνω στην γλωσσική δομή. Στις νεότερες μορφές η κρυπτογραφία κάνει χρήση του αριθμητικού ισοδύναμου, η έμφαση έχει μεταφερθεί σε διάφορα πεδία των μαθηματικών. Η κρυπτογραφία χωρίζεται χρονικά σε τρία στάδια :

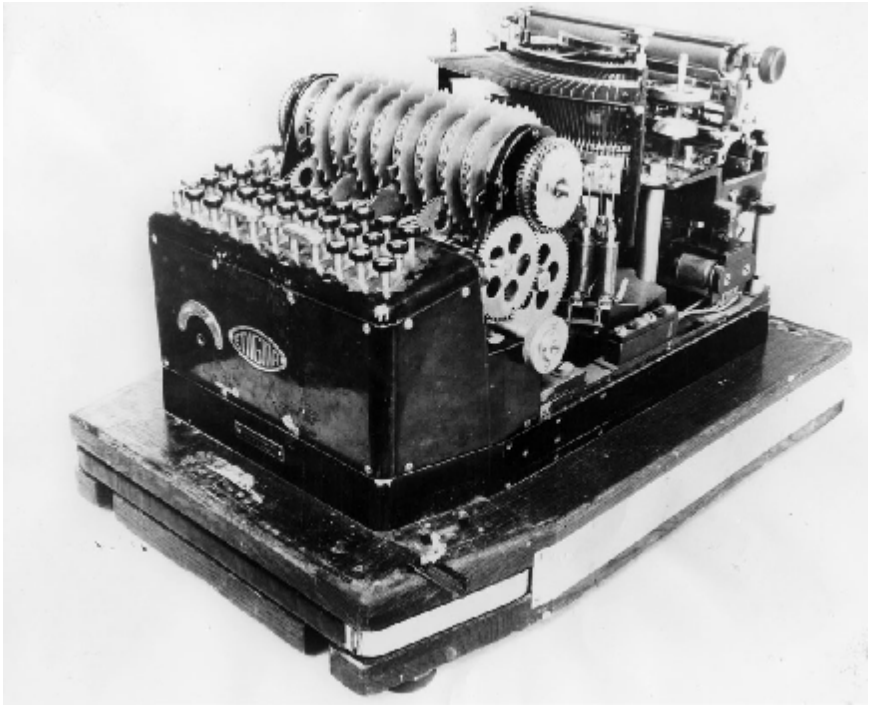
- $1^{ο}$ στάδιο: 1900 π. Χ – 1900 μ. Χ

Στο πρώτο στάδιο οι διαδικασίες αφορούσαν την έντυπη απεικόνιση. Είχαν τη μορφή αντικατάστασης και αναδιάταξης των γραμμάτων της αλφαβήτου. Το 2000 π. Χ οι ιερείς στην Αρχαία Αίγυπτο αλλοίωναν το νόημα σε ορισμένα ιερογλυφικά. Τον $5^{ο}$ αιώνα π. Χ η κρυπτογραφία χρησιμοποιείται για πρώτη φορά στον Σπαρτιατικό στρατό με τον όρο «σκυτάλη». ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα, όταν δε ξετύλιγαν τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της ανάμειξης των γραμμάτων. Το «κλειδί» ήταν η διάμετρος της σκυτάλης.



- $2^{ο}$ στάδιο: 1900 μ. Χ – 1950 μ. Χ

Σε αυτή την περίοδο αναφέρονται οι πρώτες κρυπτογραφικές μηχανές, κυρίως στην περίοδο του Β’ Παγκοσμίου Πολέμου. Ένα πολύ γνωστό σύστημα ήταν η μηχανή Enigma όπου οι Γερμανοί έκαναν εκτενή χρήση. Την λειτουργία της "έσπασε" μια ομάδα μαθηματικών, παρέχοντας έτσι σπουδαία υπηρεσία στα συμμαχικά στρατεύματα και επιταχύνοντας την έλευση της νίκης.



- 3^{o} στάδιο: 1950 μ. Χ – σήμερα

Σαν τελευταίο στάδιο θεωρείται το σύγχρονο κρυπτογραφικό σύστημα, απόρροια της αλληλεπίδρασης των μαθηματικών, της μικροηλεκτρονικής και των υπολογιστικών συστημάτων επιτρέποντας έτσι την χρήση πολυπλοκότερων αλγορίθμων. Υπάρχουν δύο μεγάλες οικογένειες αλγόριθμων, οι συμμετρικοί αλγόριθμοι (ή αλγόριθμοι μυστικού κλειδιού) και οι ασύμμετροι (ή αλγόριθμοι δημόσιου κλειδιού).

1. 2 Η Κρυπτογραφία σήμερα

Στο σύγχρονο περιβάλλον η κρυπτογραφία δεν είναι μόνο κρυπτογράφηση και αποκρυπτογράφηση. Η πιστοποίηση ταυτότητας(authentication), εκτός από τη διασφάλιση απορρήτου(privacy), είναι μια άλλη έννοια που έχει γίνει μέρος της ζωής μας καθώς γίνεται πιστοποίηση της ταυτότητας καθημερινά και ανεπαίσθητα.

Ένα παράδειγμα είναι η επίδειξη της ταυτότητα ή η υπογραφή ενός έγγραφου. Αυτό συμβαίνει καθώς ο κόσμος αλλά και η τεχνολογία εξελίσσεται ραγδαία όπου αυτό έχει σαν αποτέλεσμα οι περισσότερες συναλλαγές πλέον να γίνονται ηλεκτρονικά. Έτσι, με αυτόν τρόπο οι ηλεκτρονικές τεχνικές που θα επιτελούν την πιστοποίηση της ταυτότητας μας είναι αναπόσπαστο κομμάτι.

Η κρυπτογραφία παρέχει αυτούς τους μηχανισμούς για τη διασφάλιση των συναλλαγών. Η ψηφιακή υπογραφή είναι ένας τέτοιος μηχανισμός όπου συνδέει ένα έγγραφο με τον κάτοχο ενός κλειδιού έτσι ώστε όλοι είναι σε θέση να το αναγνώσουν να είναι σίγουροι για το ποιος το έχει γράψει. Επιπλέον, μια άλλη τέτοια διαδικασία είναι η ψηφιακή χρονοσφραγίδα (digital timestamp), που συνδέει ένα έγγραφο με την

ώρα της δημιουργίας του. Τέτοιο μηχανισμοί μπορούν να χρησιμοποιηθούν για έλεγχο πρόσβασης σε ένα σκληρό δίσκο, για ασφαλής συναλλαγές μέσω του Διαδικτύου ή ακόμα και για σύνδεση με καλωδιακή τηλεόραση.

1.3 Ορισμός Κρυπτογράφησης

Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit. Η ακολουθία bit καλείται "κλειδί" και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση. Για μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά που χρησιμοποιούνται διαφέρουν. Η διαδικασία της μπορεί να εκτελεστεί τόσο σε hardware όσο και σε software. Παρόλα αυτά η ενσωμάτωση των μεθόδων της σε hardware επιτυγχάνεται σε μεγαλύτερο βαθμό. Κάπου εδώ αξίζει να αναφερθεί πως επειδή οι χρήστες της δεν αντιλαμβάνονται την παρουσία της, αυξάνεται η αποτελεσματικότητα του εργαλείου στην παρεχόμενη ασφάλεια. Δυστυχώς όμως, λόγω του υψηλού κόστους δεν έχει καθιερωθεί σε αυτή την μορφή αφού απαγορεύει την αγορά και διατήρηση των ειδικών μηχανημάτων που χρειάζονται για την εφαρμογή της τα οποία βρίσκονται τοποθετημένα σε στρατηγικά σημεία κάθε δικτύου.

1.4 Είδη κρυπτογράφησης

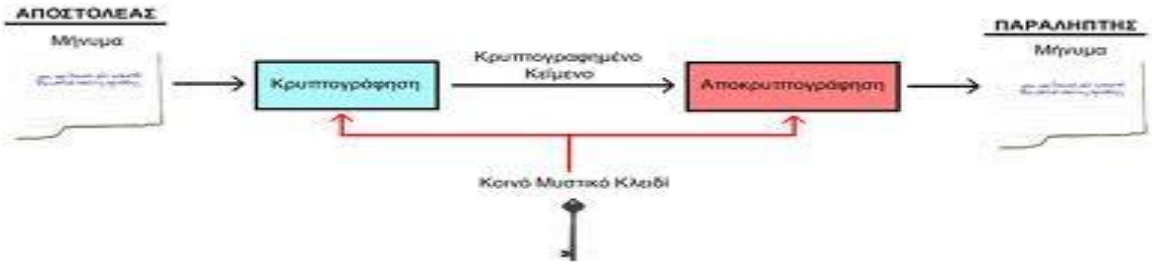
Συμμετρική κρυπτογράφηση

Όπως έχει ήδη αναφερθεί η συμμετρική κρυπτογράφηση χρονολογείται από την αρχαία Αίγυπτο αλλά ακόμα και σήμερα είναι αναπόσπαστο κομμάτι των πληροφοριακών συστημάτων. Πιο συγκεκριμένα η λειτουργία της συμμετρικής κρυπτογράφησης βασίζεται σε ένα και μόνο μυστικό κλειδί το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση. Το κλειδί αυτό θα πρέπει να το γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης προκειμένου να γραφτεί αλλά και να διαβαστεί το μήνυμα. Παρόλα αυτά η συμμετρική έχει ένα βασικό πρόβλημα. Όσο ασφαλής και αν είναι, χρειάζεται πάντα να έρθουν σε επικοινωνία ο Α με τον Β προκειμένου να δοθεί το κλειδί για την διακινούμενη πληροφορία χωρίς κάποιος άλλος να λάβει γνώση αυτού. Σημαντική λειτουργία τέτοιου είδους κρυπτογράφησης είναι η πιστοποίηση ταυτότητας, η τεχνική αυτή ονομάζεται MAC. Έτσι η ανταλλαγή κλειδιού μπορεί να γίνει με δύο τρόπους:

- Μέσω φυσικής ζεύξης, δηλαδή ανταλλαγή του κλειδιού πρόσωπο με πρόσωπο. Οι Α και Β πρέπει να συναντηθούν προκειμένου να παραδώσει ο αποστολέας το κλειδί στον παραλήπτη.
- Μέσω μιας έμπιστης τρίτης οντότητας όπου οι χρήστες την εμπιστεύονται για την ασφαλή μεταφορά του.

Πλεονεκτήματα-Μειονεκτήματα Συμμετρικής Κρυπτογραφίας

Βασικό πλεονέκτημα της μεθόδου είναι ότι είναι πιο γρήγορη συγκριτικά με την ασύμμετρη, με ταχύτητες που μπορούν να υπερβούν τα 100 Mbps. Ένα ακόμα πλεονέκτημα της είναι η μικρές απαιτήσεις της σε μνήμη αλλά και σε υπολογιστική ισχύ αφού το μέγεθος του κρυπτογραφήματος είναι μικρότερο από το αρχικό μήνυμα. Έτσι, καθίσταται δυνατή η εφαρμογή της σε κινητά τηλέφωνα αλλά και σε «έξυπνες κάρτες». Από την άλλη πλευρά όμως καθώς το πλήθος των χρηστών μεγαλώνει, μεγαλώνει και το πλήθος των κλειδιών. Αξίζει να σημειωθεί λοιπόν πως για την επικοινωνία n ατόμων απαιτούνται $n^2/2$ μοναδικά συμμετρικά κλειδιά.



Ασύμμετρη κρυπτογράφηση

Η κρυπτογραφία δημοσίου κλειδιού (public-key cryptography) αξιοποιείται κατά προτεραιότητα:

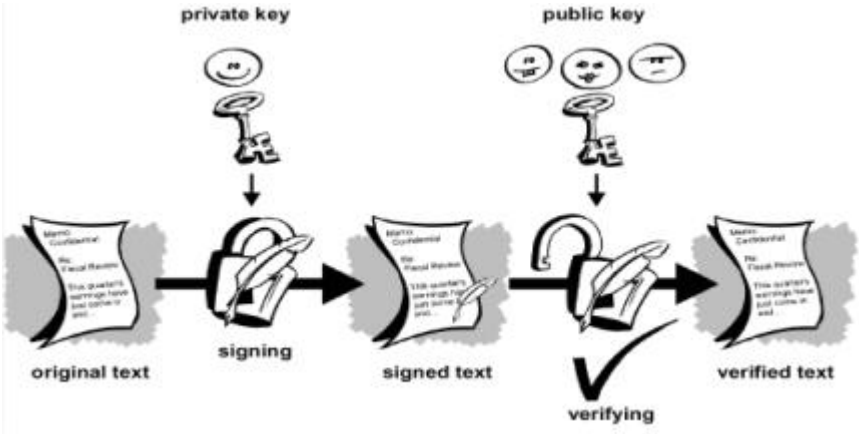
- για αυθεντικοποίηση μηνυμάτων.
- για διανομή μυστικών κλειδιών.

Η κρυπτογράφηση δημοσίου κλειδιού ή ασύμμετρου κλειδιού (Asymmetric Cryptography) δεν χρησιμοποιεί ένα κοινό κλειδί αλλά διαθέτει διαφορετικά κλειδιά για διαφορετικές λειτουργίες, χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Συγκεκριμένα, ο κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ιδιωτικό κλειδί (private key) και το δημόσιο κλειδί (public key). Το ιδιωτικό κλειδί ο κάθε χρήστης θα πρέπει να το κρατάει κρυφό ενώ αντίθετα το δεύτερο δημοσιοποιείται με αποτέλεσμα όλες οι επικοινωνίες στο δίκτυο να βασίζονται σε αυτό. Ως απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εμπιστεύσιμη συσχέτιση των δημόσιων κλειδιών με τους κατόχους τους ώστε να μην είναι δυνατή η σκόπιμη ή μη πλαστοπροσωπία. Η σχέση μεταξύ των δύο αυτών κλειδιών είναι μαθηματική(μονόδρομες συναρτήσεις).

Τυπικά, λοιπόν, είναι δυνατόν να νικηθεί ένα τέτοιο κρυπτοσύστημα ανακτώντας το ιδιωτικό κλειδί από το δημόσιο. Η επίλυση αυτού του προβλήματος είναι πολύ δύσκολη και συνήθως απαιτεί την παραγοντοποίηση ενός μεγάλου αριθμού. Η κρυπτογράφηση με χρήση της ασύμμετρης κρυπτογραφίας γίνεται ως εξής: όταν ο χρήστης Α θέλει να στείλει ένα μυστικό μήνυμα στον χρήστη Β, χρησιμοποιεί την δημόσια κλείδα του Β για να κρυπτογραφήσει το μήνυμα και έπειτα το στέλνει στον Β. Ο χρήστης Β, αφού παραλάβει το μήνυμα, κάνει χρήση της ιδιωτικής του κλείδας για να το αποκρυπτογραφήσει. Κανένας που "ακούει" την σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα. Οποιοσδήποτε έχει την δημόσια κλείδα του Β μπορεί να του στείλει μήνυμα και μόνο αυτός μπορεί να το

διαβάσει γιατί είναι ο μόνο που γνωρίζει την ιδιωτική κλείδα. Όταν ο Α θέλει να χρησιμοποιήσει την ασύμμετρη κρυπτογραφία για να υπογράψει ένα μήνυμα, τότε πραγματοποιεί ένα υπολογισμό που απαιτεί την ιδιωτική του κλείδα και το ίδιο το μήνυμα.

Το αποτέλεσμα του υπολογισμού καλείται ψηφιακή υπογραφή και μεταδίδεται μαζί με το μήνυμα. Για να επαληθεύσει την υπογραφή ο Β πραγματοποιεί ανάλογο υπολογισμό χρησιμοποιώντας την δημόσια κλείδα του Α, το μήνυμα και την υπογραφή. Εάν το αποτέλεσμα είναι θετικό, τότε η υπογραφή είναι αυθεντική. Διαφορετικά η υπογραφή είναι πλαστή ή το μήνυμα έχει τροποποιηθεί.



Πλεονεκτήματα - Μειονεκτήματα Ασύμμετρης Κρυπτογραφίας

Παρακάτω θα αναλύσουμε τα πλεονεκτήματα της ασύμμετρης κρυπτογραφίας

- Δεν χρειάζεται να υπάρχει ένας ασφαλής δίαυλος προκειμένου να μεταδοθεί για πρώτη φορά το δημόσιο κλειδί. Έτσι, αν το πρόσωπο Β υποκλέψει ή βρει το δημόσιο κλειδί του προσώπου Α, μπορεί μεν να το χρησιμοποιήσει για να στείλει στον Α ένα ιδιωτικό μήνυμα, όχι όμως για να προσποιηθεί προς τρίτους ότι είναι ο Α, ούτε για να αποκρυπτογραφήσει μηνύματα τρίτων που έχουν σταλεί στον Α κρυπτογραφημένα με το δημόσιο κλειδί του Α. Όλα αυτά συμβαίνουν γιατί το ιδιωτικό κλειδί το έχει ο Α και οι παραπάνω λειτουργίες μπορούν να αποκρυπτογραφηθούν μόνο με το ιδιωτικό του κλειδί για αυτό είναι και ο μοναδικός κάτοχος. Από τα παραπάνω προκύπτει ότι ο Α μπορεί να στείλει στον Β το δημόσιο κλειδί του είτε μέσω e-mail ή ακόμη και να το «δημοσιεύσει» σε ειδικές για το σκοπό αυτό ηλεκτρονικές υπηρεσίες καταλόγου (public key directories).

- Σε μια επικοινωνία μεταξύ των Α και Β, ο Β δεν είναι δυνατόν να επωφεληθεί από την υποκλοπή μηνυμάτων τρίτων προσώπων προς τον Α (αφού για την αποκρυπτογράφηση τους απαιτείται η γνώση του ιδιωτικού κλειδιού του Α)

αλλά ούτε και να προσποιηθεί ότι είναι ο Α. Εξάλλου η δημοσιοποίηση του δημόσιου κλειδιού του Α προς τρίτους δεν έχει κανένα νόημα, αφού (από τον σχεδιασμό του συστήματος) προορισμός του είναι ακριβώς να είναι γνωστό και διαθέσιμο σε κάθε ενδιαφερόμενο.

- Σκοπός των ασύμμετρων κλειδιών είναι να μπορεί να εξυπηρετήσει ταυτόχρονα πολλούς χρήστες. Ο κάθε χρήστης χρειάζεται να μοιραστεί με τους άλλους μόνο το δημόσιο κλειδί του. Έτσι, για να επικοινωνήσουν τέσσερα πρόσωπα (έστω τα Α, Β, Γ, Δ) μεταξύ τους, χρειάζεται να κοινοποιηθούν μόνο τέσσερα κλειδιά, ενώ για την επικοινωνία μεταξύ 100 προσώπων χρειάζεται να κοινοποιηθούν 100 κλειδιά. Αντίθετα, κατά τη χρήση συμμετρικών κλειδιών θα χρειαζόμασταν 9.900 κλειδιά. Ο αριθμός των χρησιμοποιούμενων κλειδιών είναι ανάλογος του πλήθους των συμμετεχόντων στην επικοινωνία, ενώ στα συστήματα συμμετρικής κρυπτογραφίας ο αριθμός των κλειδιών είναι ανάλογος του τετραγώνου των συμμετεχόντων. Κατά συνέπεια, οργανισμοί με μεγάλο πλήθος χρηστών δεν έχουν προβλήματα διαχείρισης υπερβολικού πλήθους κλειδιών. Όλοι όσοι χρειάζονται να στείλουν κρυπτογραφημένα μηνύματα σε ένα πρόσωπο Α, χρησιμοποιούν το ίδιο κλειδί, το δημόσιο κλειδί του Α.

- Δεν απαιτείται να έχει κανείς εκ των προτέρων κάποια σχέση με κάποιον στον οποίο θέλει να απευθύνει ένα μήνυμα κάτι το οποίο είναι απαραίτητο στα συστήματα συμμετρικού κλειδιού, προκειμένου να καταστεί δυνατή η ανταλλαγή του συμμετρικού κλειδιού, στο οποίο θα βασιστεί στη συνέχεια η αποκρυπτογράφηση. Με το σύστημα δημόσιου / ιδιωτικού κλειδιού, ο αποστολέας απλώς εντοπίζει το δημόσιο κλειδί του παραλήπτη, κρυπτογραφεί το μήνυμα και το αποστέλλει. Ο παραλήπτης διαθέτει ήδη το ιδιωτικό του κλειδί με βάση το οποίο και αποκρυπτογραφεί το μήνυμα.

- Κάθε κάτοχος ενός τέτοιου ζεύγους κλειδιών μπορεί να πραγματοποιεί μαθηματικές διεργασίες με το ιδιωτικό του κλειδί, όπου κανένας άλλος σε παγκόσμιο επίπεδο δεν είναι σε θέση να εκτελέσει. Αυτό, αποτελεί και τη βάση για τις ψηφιακές υπογραφές (digital signatures) αλλά και τη διασφάλιση της δυνατότητας της μη-αποκήρυξης (non-repudiation).

Σαφώς πέρα από τα αρκετά πλεονεκτήματα που παρουσιάζει η ασύμμετρη κρυπτογραφία έχει και αρκετά μειονεκτήματα:

- Πρώτο και βασικότερο μειονέκτημα είναι οι μεγάλες απαιτήσεις των ασύμμετρων αλγορίθμων σε επίπεδο μαθηματικών υπολογισμών συγκριτικά με τους συμμετρικούς. Αυτός είναι και ο λόγος που είναι συγκριτικά πιο αργοί, 10 έως 100 φορές, σε σχέση με τους άλλους αντίστοιχης ισχύος. Σήμερα, κάποιες από τις απαιτούμενες διαδικασίες μπορούν να διεκπεραιωθούν με τη βοήθεια ηλεκτρονικών υπολογιστών και τη χρήση κατάλληλων προγραμμάτων λογισμικού. Παρόλα αυτά η παραπάνω διαφορά αποκτά ιδιαίτερη σημασία, αν τα δεδομένα δεν είναι τα περιεχόμενα ενός μηνύματος λίγων γραμμών, αλλά πληροφορίες για ένα πολύ μεγάλο έργο, όπως π.χ. κάποιο έργο γενετικής μηχανής.

- Επιπλέον, το μέγεθος του κρυπτογραφημένου μηνύματος είναι μεγαλύτερο από το αντίστοιχο αρχικό σε έναν ασύμμετρο αλγόριθμο. Αυτό μπορεί να αποτελέσει ένα σοβαρό ζήτημα όταν χρησιμοποιούνται πολλαπλά επίπεδα κρυπτογράφησης. Π.χ. μια εφαρμογή λογισμικού που κρυπτογραφεί δεδομένα , τα οποία στη συνέχεια αποστέλλονται μέσω μιας ασφαλούς σύνδεσης Web (secure Web session) με αποτέλεσμα τα δεδομένα να φτάνουν αρκετά διογκωμένα στον παραλήπτη. Επιπρόσθετα, αν η αποστολή να γίνει μέσα από ένα κρυπτογραφημένο δίαυλο (IPSec tunnel), θα υπάρξει παραπέρα διόγκωση του μεγέθους των δεδομένων.

1.5 Συνδυασμός Ασύμμετρης και Συμμετρικής Κρυπτογράφησης

Είναι εμφανές ότι και τα παραπάνω δύο συστήματα κρυπτογραφίας παρουσιάζουν πλεονεκτήματα αλλά και μειονεκτήματα. Παρόλα αυτά όμως, υπάρχει μια συμπληρωματικότητα όσον αφορά το γεγονός ότι όπου υπερτερεί το ένα υστερεί το άλλο. Ιδανικά θα πρέπει να γίνει ένας συνδυασμός και των δύο που να εκμεταλλεύεται τα πλεονεκτήματα του καθενός, χωρίς να κληρονομεί τα αντίστοιχα μειονεκτήματα. Ένας τέτοιος συνδυασμός θα πρέπει να συγκεντρώνει τις κάτωθι ιδιότητες:

- Η προσφερόμενη λύση να είναι ασφαλής
- Η κρυπτογράφηση να είναι ταχεία
- Το κρυπτογραφημένο κείμενο να είναι συμπαγές
- Η λύση να μπορεί να επεκταθεί για την εξυπηρέτηση μεγάλων πληθυσμών
- Η λύση να μην είναι ευάλωτη ως προς την υποκλοπή του κλειδιού
- Η λύση να μην απαιτεί προϋπάρχουσα σχέση μεταξύ των δύο μερών
- Η λύση να μπορεί να υποστηρίξει ψηφιακές υπογραφές και μη-αποκήρυξη

Ο συνδυασμός αυτός μεταξύ ασύμμετρης και συμμετρικής κρυπτογράφησης δίνεται στο παρακάτω παράδειγμα:

Ο αποστολέας Α δημιουργεί ένα συμμετρικό κλειδί, το οποίο χρησιμοποιεί για την κρυπτογράφηση του μηνύματος. Το ερώτημα είναι πως θα μεταφερθεί το κλειδί αυτό στον παραλήπτη Β. Κάτι τέτοιο επιτυγχάνεται με αξιοποίηση της ασύμμετρης κρυπτογραφίας και με εντοπισμό του δημόσιου κλειδιού του παραλήπτη με τη βοήθεια κάποιου καταλόγου δημοσίων κλειδιών.

Στη συνέχεια το δημόσιο κλειδί του παραλήπτη χρησιμοποιείται για την κρυπτογράφηση του συμμετρικού κλειδιού. Βεβαίως η ασύμμετρη κρυπτογραφία είναι αργή, αλλά δεδομένου ότι το συμμετρικό κλειδί είναι πολύ μικρού μεγέθους (128bits), αυτό δεν αποτελεί πρόβλημα. Το αποτέλεσμα είναι ένα τυχαίο συμμετρικό κλειδί κρυπτογραφημένο (προστατευμένο) με τη βοήθεια ενός ασύμμετρου κλειδιού. Το τελευταίο βήμα είναι η επισύναψη του προστατευμένου συμμετρικού κλειδιού στο κρυπτογραφημένο μήνυμα, έτσι ώστε τα δύο μαζί να αποτελούν ένα αντικείμενο προς αποστολή και το οποίο είναι γνωστό ως ψηφιακός φάκελος (digital envelope). Στη συνέχει ο ψηφιακός φάκελος αποστέλλεται στον παραλήπτη μέσω του Internet. Το πρώτο βήμα μετά την παραλαβή είναι ο διαχωρισμός που περιεχομένου του ψηφιακού φακέλου και η ανάκτηση αφ' ενός του κρυπτογραφημένου μηνύματος και αφ' ετέρου του προστατευμένου συμμετρικού κλειδιού. Ο παραλήπτης χρησιμοποιεί το δικό του ιδιωτικό κλειδί για την ανάκτηση/ αποκρυπτογράφηση του συμμετρικού κλειδιού. Τέλος, με τη χρήση του συμμετρικού κλειδιού αποκρυπτογραφεί το κείμενο

του μηνύματος. Το συμμετρικό κλειδί δεν είναι πλέον χρήσιμο και μπορεί να αχρηστευτεί. Κίνδυνος υποκλοπής του μηνύματος δεν υφίσταται, ακόμη και αν κάποιος τρίτος αποκτήσει πρόσβαση στον ψηφιακό φάκελο, ενώ αυτός βρίσκεται καθ' οδόν προς τον παραλήπτη. Ο πιθανός υποκλοπέας δεν μπορεί σε καμία περίπτωση να επωφεληθεί, δεδομένου ότι θα πρέπει να λάβει γνώση του συμμετρικού κλειδιού, το οποίο όμως είναι κρυπτογραφημένο και είναι δυνατόν να αποκωδικοποιηθεί μόνο με το ιδιωτικό κλειδί του παραλήπτη, το οποίο είναι ούτως ή άλλως απόρρητο.

Παρ' όλα αυτά η μέθοδος αυτή παρουσιάζει το εξής πρόβλημα: Ένας τρίτος μπορεί να εντοπίσει το δημόσιο κλειδί του παραλήπτη Β (μέσω καταλόγου) και στη συνέχεια να δημιουργήσει ένα συμμετρικό κλειδί, με το οποίο να κρυπτογραφήσει ένα τελείως διαφορετικό μήνυμα, το οποίο και να αποστείλει στον Β με τη μορφή ψηφιακού φακέλου όπως παραπάνω. Ο Β θα παραλάβει τον ψηφιακό φάκελο, θα αποκωδικοποιήσει το συμμετρικό κλειδί με χρήση του δικού του ιδιωτικού κλειδιού και τέλος θα αποκρυπτογραφήσει το μήνυμα με το συμμετρικό κλειδί. Το μήνυμα όμως αυτό δεν έχει καμία σχέση με το πραγματικά αναμενόμενο και βεβαίως δεν έχει προέλθει από τον Α. Προκύπτει επομένως πρόβλημα πιστοποίησης της ταυτότητας του αποστολέα. Η απάντηση στο πρόβλημα αυτό μπορεί να δοθεί με τη βοήθεια των ψηφιακών υπογραφών, οι οποίες προϋποθέτουν τη χρήση των λεγομένων αλγορίθμων κατακερματισμού (hash algorithms). Τα θέματα αυτά εξετάζονται στη συνέχεια.

1.6 Κρυπτογραφία και «Πληροφοριακός Πόλεμος» των Επιχειρήσεων

Είναι γνωστό πως σε κάθε παιχνίδι άμυνας και επίθεσης, συνήθως υπάρχουν δύο παίκτες. Με τον ίδιο ακριβώς τρόπο και στις επιχειρήσεις «πληροφοριακού πολέμου», υπάρχει ένας επιθετικός αλλά και ένας αμυντικός παίχτης. Το «παιχνίδι» αυτό βασίζεται σε συγκεκριμένες πληροφοριακές πηγές, τις οποίες προσπαθεί να ανακτήσει ο επιθετικός, αλλά και σε άμυνα των πληροφοριών αυτών που προσπαθεί να προστατέψει ο αμυνόμενος. Στις περισσότερες των περιπτώσεων και ενώ ο επιτιθέμενος παίκτης θεωρείται ο «κακός» της υπόθεσης, αυτό δεν συμβαίνει όμως πάντα. Χαρακτηριστικό παράδειγμα αποτελεί ο Β' Παγκόσμιος Πόλεμος, όπου επιτιθέμενοι σε επίπεδο κρυπτογραφίας ήταν οι Σύμμαχοι που ήθελαν να σπάσουν τα κωδικοποιημένα μηνύματα των Γερμανών. Σε περιπτώσεις όμως όπου ο «πληροφοριακός πόλεμος» εξελίσσεται μεταξύ των επιχειρήσεων, τότε πρόκειται για παίκτες και πλευρές όπου μπορούν να εργάζονται μόνοι τους ή σε συγκροτημένες ομάδες.

Για να μπορέσει όμως κάποιος ο οποίος ανήκει σε κάποια επιχείρηση να αντεπιτεθεί σε κάποια άλλη με σκοπό την «κλοπή» χρήσιμων πληροφοριών, θα πρέπει φυσικά να έχει το σωστό κίνητρο, το μέσο με το οποίο θα επιτύχει κάτι τέτοιο αλλά και την κατάλληλη ευκαιρία.

Τα κίνητρα που μπορεί να έχει κάποιος για την υποκλοπή πληροφοριών, έχουν άμεση σχέση με τα ενδιαφέρονται και τα κίνητρα του ατόμου αυτού, ενώ τα μέσα που θα έχει στην διάθεση του έχουν άμεση συνάρτηση με τις ικανότητες του. Όσον αφορά την ευκαιρία που πρέπει να έχει κάποιος για να υποκλέψει και να αποκτήσει τις πηγές που επιθυμεί, θα πρέπει να αφορά την δυνατότητα πρόσβασης στις πηγές που θέλει σε συνδυασμό με κάποιο άλλο παράγοντα αλλά και την μέθοδο της κρυπτογράφησης που εφαρμόζεται στο συγκεκριμένο σύστημα .

Οι παράγοντες αυτοί σχετίζονται με την πεποίθηση που μπορεί να έχει το συγκεκριμένο άτομο ότι η ενέργεια αυτή θα επιτύχει και φυσικά ότι κανένας από τους βοηθούς του ή συνεργούς του θα συλληφθούν ή θα αποτύχουν. Αν βέβαια εντοπιστεί

να υπάρχει κάποια αρχική αδυναμία πριν από την εκτέλεση του στόχου, τότε τα άτομα που θα εμπλακούν σε μια τέτοια επιχείρηση θα πρέπει να δράσουν άμεσα και να βελτιώσουν τυχόν ελαττώματα και πιθανές απώλειες .

Κατηγορίες ομάδων υποκλοπής πληροφοριών

Σε μια επίθεση υποκλοπής πληροφοριών μπορούν να εμπλέκονται διάφορες κατηγορίες ατόμων και οργανισμών, τα οποία είναι δυνατόν να χαρακτηριστούν ως χάκερς, τρομοκράτες, εγκληματίες, κυβερνήσεις και επιχειρήσεις. Στην κατηγορία των προσώπων εμπλέκονται όλοι όσοι εργάζονται ως υπάλληλοι σε μια επιχείρηση, είτε αυτοί είναι τέως υπάλληλοι είτε εργάζονται στην εταιρεία στην παρούσα φάση. Επίσης στα πρόσωπα συγκαταλέγεται και οποιοδήποτε άλλο πρόσωπο μπορεί να έχει πρόσβαση στις πληροφορίες που επιθυμεί.

Η συγκεκριμένη αυτή ομάδα ατόμων αποτελεί και την μεγαλύτερη απειλή για τις επιχειρήσεις και τις υποκλοπές πληροφοριών από αυτές και αρκετές φορές λειτουργούν ως μεσίτες αυτών των πληροφοριών, πουλώντας αυτές σε ανταγωνίστριες εταιρείες, κυβερνητικούς παράγοντες αλλά και ξένους οργανισμούς. Γεγονός βέβαια που δημιουργεί σοβαρότατα προβλήματα σε οποιοδήποτε στρατιωτικό ή επιχειρηματικό πλάνο, τόσο στον ιδιωτικό όσο και δημόσιο τομέα και συνδέεται άμεσα με την μέθοδο της κρυπτογράφησης .

Ομάδα η οποία χαρακτηρίζεται εξίσου επικίνδυνη αφού μπορεί να προκαλέσει και εκείνη πολύ σοβαρά προβλήματα, είναι εκείνη των «χάκερς». Συνήθως η ομάδα αυτή απαρτίζεται από άτομα φανατικά προσκείμενα στους υπολογιστές και οι οποίοι διαθέτουν απεριόριστες γνώσεις γύρω από αυτούς. Ασχολούνται με τα μυστικά των «μηχανών» αυτών από πολύ μικρά παιδιά και έχουν μετατρέψει σε κερδοφόρο επάγγελμα το χόμπυ τους. Πολλά από αυτά τα άτομα εργάζονται σε κυβερνητικούς οργανισμούς και πολυεθνικές εταιρείες, αφού πολλοί πιστεύουν πως με τις γνώσεις τους μπορούν να προστατέψουν ή να παρέχουν με μυστικό τρόπο, τις πληροφορίες που χρειάζονται οι επιχειρήσεις και οι κυβερνήσεις των χωρών .

Μια άλλη κατηγορία ατόμων που ασχολούνται με τον «πληροφοριακό πόλεμο» και την κρυπτογράφηση, είναι εκείνη των εγκληματιών. «Τα συγκεκριμένα άτομα έχουν ως απώτερο σκοπό την συλλογή πληροφοριών οικονομικού περιεχομένου και σχετικά με αριθμούς πιστωτικών καρτών, αριθμούς λογαριασμών τραπεζών και δικαιωμάτων πνευματικής ιδιοκτησίας. Στην ίδια ομάδα περιλαμβάνονται και οι πωλητές «πειρατικών» CD και προγραμμάτων ηλεκτρονικών υπολογιστών .

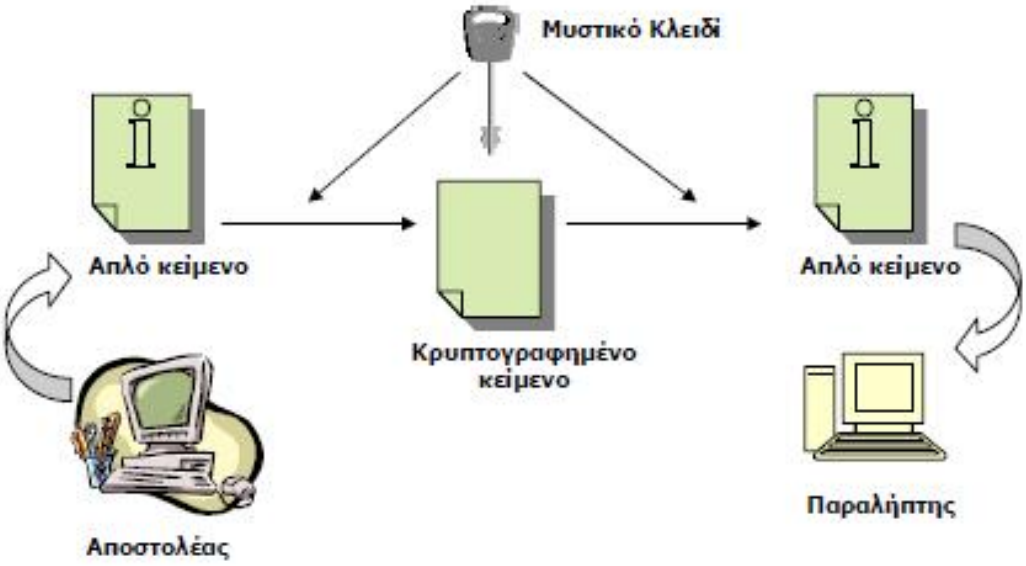
Τέλος, θα πρέπει να γίνει αναφορά και στην κατηγορία των κυβερνητικών οργανισμών και επιχειρήσεων που σχετίζονται με τον «πληροφοριακό πόλεμο» και την κρυπτογράφηση. Στην κατηγορία αυτή ανήκουν οι υπηρεσίες κατασκοπείας και η παρακολούθηση εγκληματικών πράξεων καθώς και οι ενέργειες διεθνούς κατασκοπείας. Οι τελευταίες επιδιώκουν συνήθως να αποκτήσουν κάποιες σημαντικές στρατιωτικές ή διπλωματικές πληροφορίες, σχετικά με τον έλεγχο διοικητικών και τεχνολογικών συστημάτων .

1.7 Σχέση Λειτουργίας Κρυπτογραφίας με Αλγόριθμους

Σχέση Λειτουργίας Συμμετρικής Κρυπτογραφίας με Αλγορίθμους

Το κρυπτογραφικό αυτό σύστημα είναι το πλέον γνωστό και χαρακτηρίζεται από την ύπαρξη ενός και μόνο κώδικα ή κλειδιού, το οποίο χρησιμοποιείται τόσο για την κρυπτογράφηση του μηνύματος από τον αποστολέα - πριν την αποστολή - όσο και για την αποκρυπτογράφηση του από τον παραλήπτη - μετά την μεταφορά. Για αυτό και ονομάζεται συμμετρικό. Επιπλέον είναι γνωστό και με τα ονόματα κρυπτογραφία μυστικού κλειδιού (secret key) ή και διαμοιραζομένου μυστικού (shared secret), αφού όπως έχουμε εξηγήσει το κλειδί θα πρέπει να παραμείνει μυστικό, αλλά ταυτόχρονα να είναι προσβάσιμο μόνο στα δύο μέρη που ανταλλάσσουν μηνύματα. Για τη λειτουργία λοιπόν του συστήματος με αποτελεσματικό τρόπο θα πρέπει, αποστολέας και παραλήπτης, εκ των προτέρων, να συμφωνήσουν σε ένα μυστικό κλειδί και του οποίου η λειτουργία εμφανίζεται στο ακόλουθο σχεδιάγραμμα.

Λειτουργία Συμμετρικής Κρυπτογραφίας



Τα κρυπτογραφικά κλειδιά παρουσιάζουν αρκετές ομοιότητες με τα κλειδιά της καθημερινής ζωής όπου χρησιμοποιούνται π.χ. για να κλειδώσουν ή να ξεκλειδώσουν μια πόρτα. Κάθε τύπος «κλειδαριάς», έχει ένα κλειδί ειδικού σχήματος που ταιριάζει σ' αυτήν και το οποίο πρέπει να έχει το σωστό μήκος και τη σωστή μορφολογία. Ένα κλειδί για κλειδαριές συγκεκριμένου κατασκευαστή είναι πολύ πιθανόν να ταιριάζει σε οποιαδήποτε κλειδαριά αντίστοιχου τύπου, αλλά μόνο το σωστό κλειδί, αυτό με το κατάλληλο μήκος και μορφολογία μπορεί να περιστραφεί και να ανοίξει την «κλειδαριά».

Έτσι και στα σύγχρονα συστήματα κρυπτογραφίας που λειτουργούν με χρήση υπολογιστών, κάθε κρυπτογραφικός αλγόριθμος χρειάζεται ένα κλειδί με το σωστό μήκος, δηλαδή με το σωστό αριθμό bits. Ο αλγόριθμος μπορεί να λειτουργήσει με οποιοδήποτε κλειδί έχει το κατάλληλο μήκος όμως η εφαρμογή του αλγόριθμου θα

έχει ως αποτέλεσμα την αποκρυπτογράφηση ενός κρυπτογραφημένου μηνύματος μόνο με το κλειδί που διαθέτει τη σωστή ακολουθία bits.

Οι συμμετρικοί αλγόριθμοι κρυπτογράφησης δέχονται σαν είσοδο ένα κανονικό αναγνώσιμο κείμενο (clear text- plain text) και με τη χρήση του συμμετρικού κλειδιού παράγουν σαν αποτέλεσμα (εξαγόμενο) μια κρυπτογραφημένη μορφή του αρχικού κειμένου. Το συμμετρικό κλειδί δεν είναι παρά ένα τυχαίος αριθμός με το σωστό μέγεθος. Έτσι, αν ο αλγόριθμος είναι συμμετρική κρυπτογράφηση των 40bits, το συμμετρικό κλειδί θα είναι μήκους 40bits, ενώ αν πρόκειται για αλγόριθμο συμμετρικής κρυπτογράφησης των 128 bits, τότε το συμμετρικό κλειδί θα είναι μήκους 128 bits.

Ένας κρυπτογραφικός αλγόριθμος μπορεί να χαρακτηριστεί ως ασφαλής εφ' όσον έχει προηγηθεί ο εξαντλητικός έλεγχος του από τους κρυπταναλυτές, χωρίς να εντοπισθούν αδυναμίες. Υπ' αυτές τις προϋποθέσεις ο μόνος τρόπος να παραβιαστεί ένα κρυπτογραφημένο μήνυμα, είναι να δοκιμαστούν όλες οι πιθανές τιμές κλειδιών που αντιστοιχούν στο συγκεκριμένο μέγεθος. Αυτό αποκαλείται επίθεση ωμής βίας (brute force attack). Στατιστικά θα χρειαστεί να δοκιμαστούν μόνο οι μισές από τις πιθανές τιμές του κλειδιού, προκειμένου να εντοπισθεί το σωστό κλειδί.

Κάτι τέτοιο προφανώς δεν ακούγεται πρακτικό αλλά ένας υπολογιστής υψηλής ταχύτητας είναι σε θέση να προσπαθήσει εκατομμύρια δοκιμές σε ένα δευτερόλεπτο. Αυτός είναι και ο λόγος που καθιστά το μήκος του κλειδιού σημαντικό. Για παράδειγμα, αν ένα κλειδί έχει μήκος 16 δυαδικά ψηφία (bits) καταλαβαίνουμε πως διαθέτει 216=65536 διαφορετικούς συνδυασμούς και θα υποστεί επίθεση ωμής βίας αμέσως. Ένα κλειδί μήκους 40 bits μπορεί να διαθέτει περισσότερους από 10^{12} συνδυασμούς.

Παρ' όλο που οι συνδυασμοί φαίνονται πολλοί και δύσκολα κανείς θα προσπαθούσε να τον «σπάσει», ένα κλειδί 40 bits θεωρείται αδύναμο και γι' αυτό δεν μπορούμε να του εμπιστευτούμε πολύτιμες πληροφορίες. Τα κλειδιά που χρησιμοποιούνται για να κρυπτογραφηθούν ευαίσθητες πληροφορίες είναι συνήθως 128 bits ή και μεγαλύτερα. 128 bits σημαίνει 10^{38} συνδυασμοί περισσότεροι από των αριθμό σταγόνων νερού που υπάρχει σε όλους τους ωκεανούς της Γης. Τα μεγέθη των κλειδιών επιλέγονται έτσι ώστε να είναι πρακτικά αδύνατο να δοκιμαστούν έστω και οι μισές πιθανές τιμές του κλειδιού, ακόμη και με χρήση τεράστιου αριθμού υπολογιστών, μέσα στο χρονικό διάστημα κατά το οποίο τα υπό προστασία δεδομένα πρέπει να παραμείνουν ασφαλή.

Πρακτικά λοιπόν είναι αδύνατο να προβλεφθεί με ακρίβεια η εξέλιξη της τεχνολογίας των υπολογιστών οπότε είναι απαραίτητο να γίνουν κάποιες υποθέσεις σχετικά με την πιθανή αύξηση της επεξεργαστικής τους ισχύος. Αντίστοιχα θα πρέπει να σημειωθεί πως υπάρχουν οι εξής κατηγορίες συμμετρικών αλγορίθμων κρυπτογράφησης:

- ***DES*** Είναι οι αλγόριθμοι όπου χωρίζουν τα προς κρυπτογράφηση δεδομένα σε πακέτα των 64bits και είναι γνωστοί ως "block ciphers". Ο πιο γνωστός από αυτούς είναι ο DES (Data Encryption Standard), ο οποίος έχει σταθερό μήκος κλειδιού 56bits και αναπτύχθηκε αρχικά από την IBM στην δεκαετία του 1970, ενώ στη συνέχεια υιοθετήθηκε και από την κυβέρνηση των ΗΠΑ ως το επίσημο πρότυπο κρυπτογράφησης απορρήτων πληροφοριών. Ο DES υπήρξε εν χρήσει για μεγάλο διάστημα και χρησιμοποιήθηκε σε πολλά κρυπτογραφικά συστήματα, όπως το σύστημα Kerberos, το οποίο αναπτύχθηκε στο MIT. Λόγω όμως της αυξανόμενης ισχύος των υπολογιστών το μήκος 56bits κλειδί

του αρχίζει να γίνεται ευάλωτο σε επιθέσεις τύπου ωμής βίας. Ο "κλασσικός" αλγόριθμος DES είναι πλέον ξεπερασμένος, αφού με τη χρήση ενός σύγχρονου υπολογιστή μπορεί να παραβιαστεί σχετικά εύκολα. Το πρότυπο που αναμένεται να δώσει νέα ζωή στο DES είναι το AES (Advanced Encryption Standard, Εξελιγμένο Πρότυπο Κωδικοποίησης). Στο μεταξύ, εφαρμόζοντας διάφορες τεχνικές επάνω στο DES, μπορεί να αυξηθεί σημαντικά την ασφάλειά του. Με τη μέθοδο Triple-DES, για παράδειγμα, το μήνυμα κωδικοποιείται τρεις φορές, με τρία διαφορετικά κλειδιά. Άλλες παραλλαγές του DES είναι: DESX, GDES, RDES όπου χρησιμοποιούνται μεγαλύτερα κλειδιά.

- ***RC4***. Στην κατηγορία αυτή ανήκουν οι αλγόριθμοι που δεν εφαρμόζονται σε πακέτα δεδομένων συγκεκριμένου μεγέθους (64 ή 128bits), αλλά σε ακολουθίες bits (stream ciphers).Ο πιο γνωστός από αυτούς είναι ο RC4, με κυριότερα χαρακτηριστικά του την ταχύτητα (είναι ταχύτερος από όλους της προηγούμενος κατηγορίας) και την υποστήριξη κλειδιών μεταβλητού μήκους.

- ***IDEA***. Ο Διεθνής Αλγόριθμος Κρυπτογράφησης Δεδομένων (International Data Encryption Algorithm), είναι δημοφιλής στην Ευρώπη αλλά όχι τόσο στην Αμερική. Με ένα μυστικό κλειδί 128 bits, θεωρείται ότι είναι πιο ασφαλής από τον DES. Ο IDEA είναι από τους βασικότερους αλγορίθμους στο λογισμικό κρυπτογράφησης του ηλεκτρονικού ταχυδρομείου, του PGP (Pretty Good Privacy). Ο άλλος είναι ο RSA που αναλύεται παρακάτω.

Τέλος, κοινές σε όλους τους συμμετρικούς αλγόριθμους είναι οι εξής ιδιότητες:

- Είναι γενικά γρήγοροι στην εκτέλεσή τους.
- Είναι συμπαγείς, με την έννοια ότι το παραγόμενο κρυπτογραφημένο μήνυμα έχει γενικά το ίδιο μέγεθος με το αρχικό μήνυμα.
- Με βάση τα παραπάνω, εάν δύο πρόσωπα Α και Β θέλουν να επικοινωνήσουν και έστω ότι ο Α επιθυμεί να στείλει ένα μυστικό μήνυμα στον Β, θα πρέπει να κινηθούν ως εξής:

- Επιλέγεται ένας συμμετρικός αλγόριθμος
- Επιλέγεται το συμμετρικό κλειδί
- Το κλειδί πρέπει να γίνει γνωστό και στους δύο: εάν το έχει επιλέξει ο Α, θα πρέπει να το αποστείλει εκ των προτέρων στον Β
- Ο Α κρυπτογραφεί το μήνυμα με τη χρήση του κλειδιού
- Ο Α αποστέλλει το κρυπτογραφημένο μήνυμα στον Β
- Ο Β αποκρυπτογραφεί το μήνυμα

Η συμμετρική κρυπτογραφία χαρακτηρίζεται από την απλότητά της, δεδομένου ότι απαιτεί την ύπαρξη ενός μόνο κλειδιού. Παρουσιάζει όμως ορισμένα σημαντικά προβλήματα. Πρέπει να υπάρχει ένας ασφαλής δίαυλος για την αρχική μεταφορά του μυστικού κλειδιού. Αν το μυστικό κλειδί υποκλαπεί, τότε όλες οι επόμενες επικοινωνίες θα είναι επισφαλείς. Βασική προϋπόθεση επιτυχούς

λειτουργίας είναι η ύπαρξη αμοιβαίας εμπιστοσύνης μεταξύ των δύο μερών. Όταν ένα συμμετρικό κλειδί αποκαλυφθεί, αυτό και κάθε μήνυμα που το χρησιμοποίησε για να κρυπτογραφηθεί έχει χάσει τα προνόμιά του. Ένα νέο κλειδί πρέπει να επιλεγεί και να διανεμηθεί.

Τα πράγματα δυστυχώς όμως δυσκολεύουν, αν ληφθεί υπ' όψη η αρχή της μη χρησιμοποίησης του ίδιου κλειδιού για παραπάνω από μια επικοινωνίες, έστω και αν αυτές γίνονται με το ίδιο πρόσωπο, δεδομένου ότι τότε αυξάνουν οι κίνδυνοι υποκλοπής του. Τέλος, σε σχέση με τις βασικές αρχές ασφάλειας που προαναφέρθηκαν στην εισαγωγή, η συμμετρική κρυπτογραφία δεν διασφαλίζει την επιβεβαίωση, αλλά ούτε και την μη αποκήρυξη. Κάθε ένα από τα δύο μέρη έχει τη δυνατότητα να τροποποιήσει κακοβούλως τα δεδομένα (ενός μηνύματος ή μιας συναλλαγής), έχοντας συγχρόνως τη βεβαιότητα ότι ένας τρίτος δεν θα είναι σε θέση να προσδιορίσει τον ένοχο.

Σήμερα χρησιμοποιεί κλειδιά μήκους τουλάχιστον 1024bits και είναι πιθανόν ο πιο πολύπλοκος και απαιτητικός σε υπολογιστική ισχύ από όλους τους εν χρήσει κρυπτογραφικούς αλγορίθμους. Επίσης πολύ γνωστός είναι ο αλγόριθμος ελλειπτικών καμπυλών (Elliptic curve cryptography- ECC), ο οποίος είναι σχετικά πιο πρόσφατος. Είναι λιγότερο πολύπλοκος και απαιτητικός σε σχέση με τον RSA και μπορεί να χρησιμοποιήσει μικρότερου μήκους κλειδιά, επιτυγχάνοντας το ίδιο επίπεδο ασφάλειας με τον RSA. Για να γίνει πιο κατανοητή η σημασία του μήκους των κρυπτογραφικών κλειδιών σε σχέση με το επιδιωκόμενο επίπεδο ασφάλειας, παρατίθεται ο πιο κάτω πίνακας, στον οποίο απεικονίζονται συγκριτικά τα μήκη κλειδιών (σε bits) των διαφόρων αλγορίθμων, σε συνδυασμό με τον χρόνο που απαιτείται προκειμένου να επιτευχθεί η παραβίαση ("σπάσιμο") του κλειδιού. Η υπόθεση που έχει γίνει είναι ότι υπάρχει διαθέσιμο ποσό 10 εκατ. δολαρίων για αγορά εξοπλισμού (υπολογιστών) και ότι η μνήμη κοστίζει περίπου 0.5 δολάρια ανά MB.

Χαρακτηριστικά Στοιχεία Συμμετρικών και Ασύμμετρων Κλειδιών

Συμμετρικό κλειδί DES	Ασύμμετρο κλειδί ECC	Ασύμμετρο κλειδί RSA	Απαιτούμενος χρόνος I	Πλήθος Μηχανών	I Μνήμη
56	112	420	5 λεπτά	10.000	Ελάχιστη
80	160	760	600 μήνες	4.300	4 GB
96	192	1020	3 εκατ. Έτη	114	170 GB
128	256	1620	1016 έτη	0,16	120 TB

Από τον πίνακα αυτό μπορεί να γίνει αντιληπτό γιατί αρχίζει να εγκαταλείπεται ο αλγόριθμος DES με υποχρεωτικό σταθερό μήκος κλειδιού 56 bits, καθώς και γιατί τα προτιμητέα μήκη κλειδιών στον αλγόριθμο RSA είναι πλέον 1024 και άνω. Εδώ θα άξιζε να αναφερθεί ότι όλοι οι κατασκευαστές λογισμικού ασύμμετρης κρυπτογράφησης υποστηρίζουν πολλαπλούς αλγόριθμους. Έτσι αν κάποια στιγμή βρεθεί ένα αδύνατο σημείο σε κάποιο αλγόριθμο, το οποίο επιτρέπει την παραβίασή του, υπάρχει πάντα η επιλογή της ενεργοποίησής ενός άλλου εναλλακτικού αλγορίθμου, ο οποίος να είναι ασφαλής.

Σχέση Λειτουργίας Ασύμμετρης Κρυπτογραφίας με Αλγορίθμους

Ένας από τους πιο διαδεδομένους και περισσότερο χρησιμοποιημένους αλγόριθμους στην κρυπτογραφία δημόσιου κλειδιού είναι ο RSA. Τον πρότειναν το 1978 ο Ron River, ο Adi Shamiy και ο Len Adleman. Αυτός ο αλγόριθμος είναι κατάλληλος για:

- Κρυπτογράφηση και αποκρυπτογράφηση δεδομένων.
- Ασφάλεια κρυπτογραφικού συστήματος.
- Ψηφιακά πιστοποιητικά. Είναι ένα έγγραφο το οποίο πιστοποιεί την αυθεντικότητα των δημόσιων κλειδιών των χρηστών με αποτέλεσμα να χρησιμοποιείται στην κρυπτογραφία δημόσιου κλειδιού. Όσον αφορά την εγκυρότητα του, πρέπει να είναι υπογεγραμμένο από κάποια Αρχή Πιστοποίησης και να περιλαμβάνει μια ημερομηνία λήξης ή Περίοδο Ισχύος.
- Ψηφιακές υπογραφές. Είναι μια σειρά συμβόλων η οποία συνοδεύει αρχεία ή ηλεκτρονικά δεδομένα και μπορεί να χρησιμοποιηθεί για την επαλήθευση της ακεραιότητας τους καθώς και για τον καταλογισμό ευθύνης (Non Repudiation).

Ο RSA στηρίζει την ασφάλειά του στη δυσκολία παραγοντοποίησης μεγάλων αριθμών.

Πλεονεκτήματα RSA

Ο RSA παρέχει πλεονεκτήματα τα οποία βοήθησαν στην ασφαλέστερη αλλά και στην ευκολότερη διαχείριση συναλλαγών.

- Απλοποίηση του προβλήματος της διαχείρισης κλειδιών.Στην ασύμμετρη κρυπτογραφία κάθε χρήστης χρειάζεται δύο κλειδιά έστω ν. Έτσι ο απαιτούμενος αριθμός κλειδιών είναι απλά 2ν. Αντίθετα στην συμμετρική ο αριθμός κλειδιών που απαιτείται είναι ν^2. Είναι κατανοητό ότι σε ένα κρυπτοσύστημα δημόσιου κλειδιού η σχέση που συνδέει τον αριθμό των κλειδιών με τους χρήστες είναι γραμμική.

- Επιπρόσθετη ασφάλεια στις συναλλαγές. Ο κάθε χρήστης χρησιμοποιεί για δική του χρήση ένα ζεύγος κλειδιών (ιδιωτικό – δημόσιο). Το ιδιωτικό θα πρέπει να μείνει κρυφό και μυστικό από οποιαδήποτε μη εξουσιοδοτημένη οντότητα ώστε να είναι ασφαλής η εγκατάσταση επικοινωνίας και να εξαλειφθεί το πρόβλημα της μεταφοράς του μηνύματος. Το δημόσιο κλειδί από την άλλη είναι περισσότερο διαδεδομένο και ευρέως διαθέσιμο με αποτέλεσμα να μπορεί να μεταφέρεται με οποιαδήποτε μέθοδο στο δίκτυο και χωρίς να υπάρχει πρόβλημα για την διατήρηση της μυστικότητας του.

Κεφάλαιο Δεύτερο: Εφαρμογές της Κρυπτογραφίας στις Οικονομικές Συναλλαγές

Για αυτό το κεφάλαιο χρησιμοποιήθηκε η εξής βιβλιογραφία:[4],[5],[12],[13],[16],[22],[23][24],[25],[29],[30],[31]

2.1 Πιστοποίηση Ταυτότητας και Ψηφιακές Υπογραφές

Στην ασύμμετρη κρυπτογραφία, σύμφωνα με τον ρόλο του δημόσιου κλειδιού το κύριο ζήτημα είναι το πώς θα διανεμηθεί το κλειδί αυτό δηλαδή ποιος είναι ο μηχανισμός αυτών των κλειδιών. Ο μηχανισμός αυτός δεν μπορεί παρά να στηρίζεται στην σύνδεση με ένα δημόσιο κλειδί το οποίο να παρέχει συγκεκριμένες πληροφορίες ώστε να προσδιορίζεται η ταυτότητα του κατόχου του. Ο συνδυασμός αυτός δημιουργεί τη λεγόμενη "ψηφιακή ταυτότητα" (digital identity) ή όπως είναι πιο γνωστό, το "ψηφιακό πιστοποιητικό" (digital certificate). Τα ψηφιακά πιστοποιητικά σχετίζονται άρρηκτα είναι δηλαδή ανάλογα με τις κλασσικές ταυτότητες και αποτελούν την βάση για τη δημιουργία ενός ασφαλούς ηλεκτρονικού περιβάλλοντος, διότι σου εξασφαλίζουν ένα σημείο εμπιστοσύνης σχετικά με το ποιος είναι ο κάτοχος ενός δεδομένου δημόσιου κλειδιού.

Για παράδειγμα, παίρνοντας το δημόσιο κλειδί ενός ατόμου Χ από κάποιο ηλεκτρονικό κατάλογο για να σταλούν κρυπτογραφημένα μηνύματα, να μην μπορούν άλλοι εκτός από αυτόν να τα βλέπουν αφού αυτός θα έχει το αντίστοιχο μυστικό κλειδί. Για να γίνει όμως αυτό θα πρέπει να είναι γνωστό ότι το κλειδί που έχει επιλεχθεί ανήκει όντως στον Χ. Ωστόσο υποθέτοντας ότι ένας Hacker (cracker)γνωρίζει τα στοιχεία του Χ τότε είναι πολύ πιθανόν να έχει βάλει το δικό του δημόσιο κλειδί στην θέση του Χ.

Έτσι κάθε φορά που θα γίνεται αποστολή ενός mail πχ στην διεύθυνση name@.com ο Hacker θα μπορεί να υποκλέπτει και να τα διαβάζει αφού θα έχει κρυπτογραφήσει το δημόσιο κλειδί. Σαν ένα συμπέρασμα από το παραπάνω παράδειγμα προκύπτει ότι ένα σύστημα κρυπτογράφησης από μόνο του δεν είναι τόσο χρήσιμο, εάν δεν υπάρχει και μια υπεύθυνη αρχή (ή αρχές) διαχείρισης των δημόσιων κλειδιών. Μια τέτοια αρχή θα πρέπει να είναι σε θέση να διασφαλίζει ότι το δημόσιο κλειδί δ1 αντιστοιχεί στο χρήστη χ1, το δημόσιο κλειδί δ2 στο χρήστη x2 κ.λπ. Η αντιστοίχηση ενός χρήστη στο δημόσιο κλειδί του παρέχεται από ένα πιστοποιητικό.

Τα πιστοποιητικά αυτά τα διανέμει η Αρχή Πιστοποίησης (certification authority or CA) η οποία δεν είναι κάτι άλλο από μια έμπιστη εταιρεία ή οργανισμό. Μια τέτοια αρχή είναι υπεύθυνη για την ανάκλαση, την δημιουργία και γενικά για την διαχείριση των πιστοποιητικών. Έτσι, εάν ο Χ επιθυμεί ένα πιστοποιητικό, αρχικά θα απευθυνθεί σε μια Αρχή Πιστοποίησης, όπως είναι η VeriSign. Η Αρχή θα ελέγξει με κάποιον τρόπο την ταυτότητα του Α, καθώς και ότι το δημόσιο κλειδί δ που προσκομίζει του ανήκει πραγματικά.

Ακολουθεί η σύνταξη ενός κειμένου, το οποίο θα περιλαμβάνει στοιχεία που αφορούν τον Χ (π.χ., ονοματεπώνυμο, διεύθυνση κατοικίας, e-mail κ.λπ.), το κλειδί, καθώς και άλλα χρήσιμα στοιχεία, όπως, π.χ., η ημερομηνία κατά την οποία η ισχύς του πιστοποιητικού εκπνέει (expiration date). Επί πρόσθετα, η Αρχή Πιστοποίησης υπογράφει το έγγραφο με το δικό της μυστικό κλειδί, δημιουργώντας έτσι το

πιστοποιητικό του Χ. Τώρα, εάν χρειαστεί κάποιος το δημόσιο κλειδί του Χ, καθώς και να επιβεβαιώσει ότι είναι δικό του, τότε παίρνει πρώτα το πιστοποιητικό του Χ από έναν κατάλογο on-line. Επαληθεύεται η ψηφιακή υπογραφή της Αρχής Πιστοποίησης και αν είναι εντάξει, τότε είναι τελικά βέβαιος ότι το κλειδί που πήρε πράγματι ανήκει στον Χ.

Συνοψίζοντας, λέγεται ότι οι χρήστες εμπιστεύονται μια αρχή πιστοποίησης γιατί κάποιος άλλος φορέας έχει εγγυηθεί για την αξιοπιστία της, όπου και για εκείνον κάποιος άλλος έχει εγγυηθεί κ.ο.κ. Υπάρχει λοιπόν, μια αλυσίδα εμπιστοσύνης (chain of trust), στη ρίζα της οποίας (root) υπάρχει μια καθολικά αποδεκτή Αρχή. Ένα σύστημα κρυπτογράφησης αρκετά γνωστό και διαδεδομένο το οποίο αναπτύχθηκε στην Αμερική το 1991 είναι το PGP(Pretty Good privacy) από τον τότε μηχανικό λογισμικού Φιλ Τσιμερμαν.

Μέχρι το 1999, η εξαγωγή κρυπτογραφικού υλικού σε ηλεκτρονική μορφή εκτός της χώρας απαγορευόταν, αφού οι τεχνολογίες του είδους είχαν χαρακτηριστεί "πυρομαχικά". Ωστόσο, χάρη στην εθελοντική πρωτοβουλία PGP International (εν συντομία PGPi), το πρόγραμμα διαδόθηκε ευρέως σε ολόκληρο τον κόσμο, ήδη από το 1997. Κάθε καινούργια έκδοση του PGP όταν κυκλοφορούσε στην Αμερική οι άμεσα ενδιαφερόμενοι δηλαδή αυτοί που συμμετείχαν στην πρωτοβουλία αγόραζαν κατευθείαν από την Αμερική τα βιβλία και τα προωθούσαν στην Ευρώπη. Στη συνέχεια, τα βιβλία σαρώνονταν σελίδα προς σελίδα, περνούσαν από πρόγραμμα OCR, και όταν ο πηγαίος κώδικας είχε μεταφερθεί ολόκληρος στον υπολογιστή, μεταγλωττίζονταν.

Σήμερα στις ΗΠΑ δεν είναι τόσο έντονες οι εξαγωγές κρυπτογραφικού υλικού και αυτό έχει σαν αποτέλεσμα το PGP να μπορεί να εξάγεται και σε ηλεκτρονική μορφή χωρίς όμως αυτό να σημαίνει ότι το Project αυτό θα σταματήσει να έχει τον έλεγχο της διανομής εκδόσεων του προγράμματος και στον υπόλοιπο κόσμο, μαζί βέβαια και με τον πηγαίο κώδικα.

Θα πρέπει να γίνει επιλογή αν θα σταλεί το δημόσιο κλειδί του κατόχου σε κάποιο διακομιστή κλειδιών, ώστε άλλοι χρήστες να μπορούν εύκολα να το πάρουν και να του στέλνουν κρυπτογραφημένα δεδομένα. Διαφορετικά αν θέλει να διανέμει το κλειδί στα άτομα που τον ενδιαφέρουν, μπορεί απλά να το επισυνάψει στα e-mail που θα τους στείλει. Πάντως, ακόμα και αν δεν στείλει άμεσα το δημόσιο κλειδί του σε κάποιο διακομιστή, μπορείτε να το κάνει αργότερα. Το PGP για Windows έρχεται μαζί με κατάλληλο plug-in, ώστε να συνεργάζεται με το Outlook. Εκεί μπορεί να υλοποιηθεί το πρώτο e-mail το οποίο θα είναι κρυπτογραφημένο και υπογεγραμμένο.

Αφού δημιουργηθεί το ζεύγος κλειδιών, μια καλή ιδέα είναι η εξαγωγή (export) του δημοσίου κλειδιού σε ένα αρχείο κειμένου, ώστε να μπορεί να το διανέμει ο χρήστης εύκολα. Αρκεί να επιλέξει το χρήστη που τον ενδιαφέρει για παράδειγμα τον ίδιο τον κάτοχο, να κάνει δεξί κλικ και να πατήσει στο Export. Την πρώτη φορά που θα κλείσετε το παράθυρο "PGPkeys", το πρόγραμμα θα τον προτρέψει να αποθηκεύσετε το ζεύγος κλειδιών που μόλις δημιούργησε σε ένα ασφαλές μέρος: «αν έπειτα από "χτύπημα" του δίσκου χάσετε το ζεύγος κλειδιών, τότε τα δεδομένα που έχουμε σε κρυπτογραφημένη μορφή θα σας είναι παντελώς άχρηστα».

Κατά τη διαδικασία εξαγωγής, παρατηρείται να γίνεται λόγος για δύο δακτυλίους κλειδιών (key ring): τον ιδιωτικό και το δημόσιο. Στον ιδιωτικό κρατούνται όλα τα ιδιωτικά κλειδιά που έχει στην κατοχή του ο χρήστης, ενώ στο δημόσιο όλα τα δημόσια (ανήκουν σε άλλους χρήστες). Σε πολλές περιπτώσεις έχει νόημα να διαθέσει περισσότερα από ένα ζεύγη κλειδιών. Το ένα θα το χρησιμοποιεί, π.χ., για την προσωπική του αλληλογραφία και το άλλο για την επαγγελματική, όπου

κατά πάσα πιθανότητα τα χρησιμοποιούμενα κλειδιά θα έχουν μεγαλύτερο μήκος (σε bit), επομένως είναι και δυσκολότερο να παραβιαστούν.

Διαδικασία ψηφιακών υπογραφών

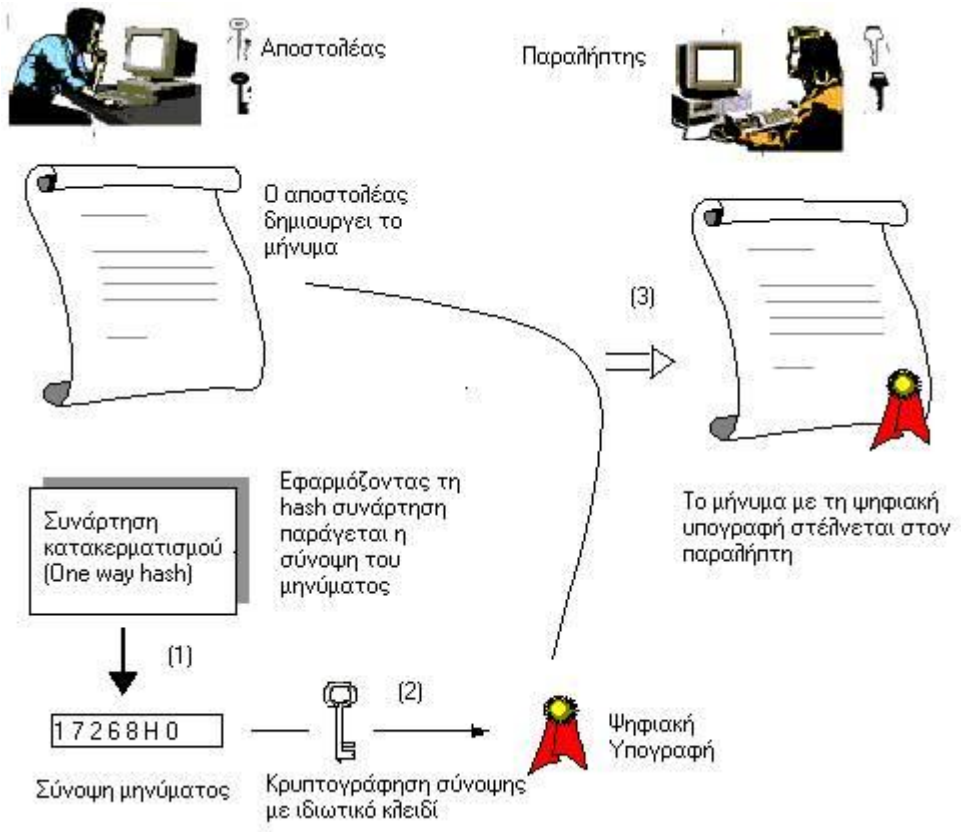
Ενώ τα πλεονεκτήματα στην ασύμμετρη κρυπτογραφία είναι πάρα πολλά, υπάρχει ένα σοβαρό ζήτημα που έχει τεθεί το οποίο χρήζει ιδιαίτερης αντιμετώπισης. Υποθέτοντας ότι λαμβάνει ο χρήστης ένα e-mail με κάποιο μήνυμα ή αρχείο από παραλήπτη με ηλεκτρονική διεύθυνση name@company.com. Υπό φυσιολογικές συνθήκες δεν έχει κανέναν λόγο να πιστέψει πως αυτός ο οποίος του έχει αποστείλει το συγκεκριμένο e-mail δεν είναι ο πραγματικός κάτοχος αυτής της διεύθυνσης. Παρόλα αυτά όμως ένας κακόβουλος χρήστης προκειμένου να βλάψει τον υπολογιστή του μέσω προγραμμάτων (E-mail facker) μπορεί να μπει στη συγκεκριμένη διεύθυνση και να σας στείλει e-mail.

Δηλαδή, να προβεί σε ηλεκτρονική πλαστοπροσωπία προσπαθώντας να σας βλάψει. Στην περίπτωση των επιχειρήσεων μπορεί να είναι κάποιος ανταγωνιστής που σκοπό έχει να του αποσπάσει επιχειρηματικά μυστικά. Άρα το πρόβλημα έγκειται στο να μάθει αν ο αποστολέας είναι όντως ο νόμιμος κάτοχος της εκάστοτε διεύθυνσης.

Αυτό το πρόβλημα μπορεί εύκολα να λυθεί με τη χρήση των ψηφιακών υπογραφών, οι οποίες είναι ισοδύναμο των χειρόγραφων υπογραφών. Οι ψηφιακές υπογραφές μπορούν να πιστοποιήσουν την σχέση ανάμεσα σε αυτόν που υπογράφει αλλά και στη σχέση του με το έγγραφο που αποστέλλει. Με άλλα λόγια, μια ψηφιακή υπογραφή είναι ορισμένα δεδομένα που συνοδεύουν ή συσχετίζονται λογικά με ένα ψηφιακά κωδικοποιημένο μήνυμα και τα οποία μπορούν να χρησιμοποιηθούν ανά πάσα στιγμή προκειμένου να εξακριβωθεί αν ο αποστολέας είναι ο νόμιμος κάτοχος της ηλεκτρονικής διεύθυνσης αλλά και για να διαπιστώσουμε πως το περιεχόμενο του μηνύματος δεν έχει αλλοιωθεί.

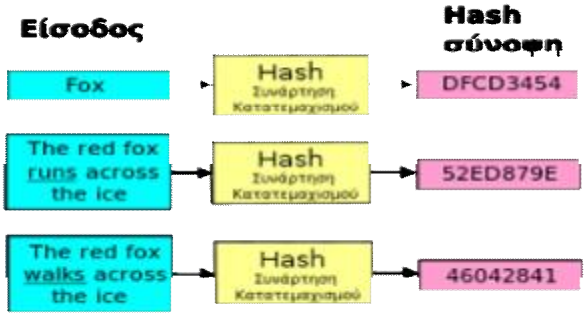
Όπως αναφέρθηκε και παραπάνω η ψηφιακή υπογραφή είναι μια μαθηματική διαδικασία η οποία έχει κάποια συγκεκριμένα χαρακτηριστικά. Η χρήση της γίνεται με τη βοήθεια της ασύμμετρης κρυπτογραφίας όπου έχει ήδη αναφερθεί η κρυπτογράφηση και αποκρυπτογράφηση στηρίζονται σε διαφορετικά κλειδιά. Μια ψηφιακή υπογραφή λοιπόν, είναι το μέσο προκειμένου ο παραλήπτης να σιγουρευτεί πως το περιεχόμενο του μηνύματος δεν είναι αλλοιωμένο.

Δημιουργία ψηφιακής υπογραφής



Οι παραπάνω διεργασίες γίνονται από το ανάλογο λογισμικό στον υπολογιστή του χρήστη.

Αυτές οι συναρτήσεις αφορούν μηχανισμούς οι οποίοι δέχονται ένα μήνυμα οποιουδήποτε μεγέθους και με τη χρήση των μαθηματικών, στην έξοδο τους δίνουν ένα αλφαριθμητικό σταθερού μήκους. Αυτό που αποτελεί ιδιαίτερο ενδιαφέρον σε αυτές τις συναρτήσεις είναι η εξαιρετική ευαισθησία που μπορεί να έχουν στα αλφαριθμητικά. Ακόμα και το παραμικρό γράμμα ή η χρήση κεφαλαίων-μικρών μπορεί να αλλάξει τη αλφαριθμητική σειρά σημαντικά. Εφαρμόζοντας, για παράδειγμα, μια συνάρτησης hash στο αλφαριθμητικό "e-banking" ο χρήστης παίρνει ως αποτέλεσμα το αλφαριθμητικό 8966f01c4a3f9a06ac 9dc99c658fe0c8, ενώ της λέξης "e-Banking" (κεφαλαίο "B") είναι το 4fa944c3c8520f5b6edc0516e7065f08 εντελώς διαφορετικά!



Δημιουργία σύνοψης/digest με την συνάρτηση κατατεμαχισμού hash function: Μικρές αλλαγές στην είσοδο δημιουργούν νέες συνόψεις.

Αξίζει να σημειωθεί ότι, αν και θεωρητικά είναι δυνατόν να δοθεί σε μια συνάρτηση hash δύο διαφορετικά μηνύματα και να γίνει λήψη του ίδιου αλφαριθμητικού, στην πράξη είναι αστρονομικά απίθανο να βρεθεί ένα τέτοιο ζεύγος μηνυμάτων εισόδου. Οι αλγόριθμοι hash που χρησιμοποιεί η κρυπτογραφία σχεδιάζονται έτσι ώστε να διαθέτουν ορισμένες ειδικές ιδιότητες τις οποίες και θα αναφερθούν παρακάτω:

- Ο αλγόριθμος δεν μπορεί να εκτελεστεί με αντίστροφη κατεύθυνση και να αποκαλύψει έστω και μέρος του αρχικού μηνύματος
- Ο αλγόριθμος δεν παρουσιάζει συγκρούσεις (collisions): έτσι είναι υπολογιστικά αδύνατη η ύπαρξη δύο διαφορετικών μηνυμάτων με το ίδιο αποτύπωμα.
- Το προκύπτον αποτύπωμα (digest) δεν αποκαλύπτει τίποτα σε σχέση με το αρχικό μήνυμα.
- Είναι πρακτικά αδύνατο να δημιουργηθεί / ανακαλυφθεί κείμενο, το οποίο να παράγει ένα συγκεκριμένο επιθυμητό αποτύπωμα. Αυτό εμποδίζει οποιονδήποτε τρίτο να υποκαταστήσει ένα μήνυμα χωρίς να προκαλέσει ασυμφωνία στο αποτύπωμα.

Οι πιο γνωστοί αλγόριθμοι που χρησιμοποιούνται για αυτή τη μετατροπή είναι ο MD5 της RSA, ο οποίος παράγει αποτύπωμα (digest) μεγέθους 128 bits και προορίζεται για χρήση σε επεξεργαστές 32-bits (σε αντίθεση με τον παλαιότερο MD2, που είχε αναπτυχθεί για χρήση σε επεξεργαστές 8-bits) και ο SHA-1 (Secure Hash Algorithm), με αποτύπωμα 160bits και ο οποίος απευθύνεται επίσης σε σύγχρονους μεγάλης ισχύος επεξεργαστές.

Πώς όμως υλοποιούνται οι ψηφιακές υπογραφές; Αν υποτεθεί ότι ο κάτοχος της διεύθυνσης name@company.com θέλει να στείλει ένα μήνυμα (έστω M) και ο παραλήπτης να είναι βέβαιος ότι προήλθε από εκείνον και όχι από κάποιον ανταγωνιστή που στόχο έχει να βλάψει την επιχείρηση του.Τότε ο ιδιοκτήτης της υπό συζήτηση ηλεκτρονικής διεύθυνσης, δεν έχει παρά να υπογράψει το M. Έτσι, τροφοδοτεί αρχικά το μήνυμα σε μια συνάρτηση hash, έστω h, παίρνοντας στην έξοδο το αλφαριθμητικό h(M), τη λεγόμενη σύνοψη μηνύματος (message digest, μπορούμε να το θεωρούμε ως δακτυλικό αποτύπωμα). Στη συνέχεια, ο αποστολέας κρυπτογραφεί το h(M) με το μυστικό του κλειδί μ, λαμβάνοντας έτσι το ciphertext s=p(h(M)). Στην ουσία, ο αποστολέας μόλις δημιούργησε την υπογραφή s του μηνύματος M που πρόκειται να αποστείλει, την οποία και θα επισυνάψει στο e-mail (θα αποστείλει, δηλαδή, το ζεύγος <M, s>).

Όταν ο παραλήπτης το λάβει, για να επικυρώσει την ταυτότητα του αποστολέα, αρχικά βρίσκει το δημόσιο κλειδί του αποστολέα, το δ. Στη συνέχεια, χρησιμοποιώντας την ίδια συνάρτηση h, υπολογίζει το h(M) και το συγκρίνει με το δ(μ(h(M))), που δεν είναι τίποτα άλλο από τη σύνοψη του μηνύματος που του έστειλε ο αποστολέας (από τη στιγμή που αποστολέας και παραλήπτης χρησιμοποιούν το ίδιο σύστημα κρυπτογράφησης, η συνάρτηση h δεν αλλάζει). Εάν ισχύει h(M)=δ(s), ο παραλήπτης δέχεται την υπογραφή ως έγκυρη. Σε διαφορετική περίπτωση συμπεραίνει ότι η υπογραφή s δεν είναι του αποστολέα, καθώς και ότι το μήνυμα M μεταβλήθηκε καθ' οδόν. Με την παραπάνω διαδικασία ο παραλήπτης βεβαιώνεται για τρία πράγματα.

- Πρώτον, ότι το e-mail προήλθε από τον συγκεκριμένο αποστολέα, αφού μόνο εκείνος θα μπορούσε να υπολογίσει την υπογραφή s, καθώς είναι ο μοναδικός κάτοχος του μυστικού κλειδιού μ.
- Δεύτερον, από τη στιγμή που ο αποστολέας υπόγραψε το μήνυμα Μ, αυτό δεν θα μπορούσε να αλλάξει στο παραμικρό, αφού τότε θα άλλαζε και το h(M) που θα υπολόγιζε ο παραλήπτης, επομένως η υπογραφή s θα ήταν άκυρη (h(M^(s)).
- Τρίτον, ο αποστολέας δεν μπορεί να ισχυριστεί ότι δεν τα έγραψε, αφού ανά πάσα στιγμή μπορούν να του δείξουν ότι h(M)=δ(s) (αρκεί, βεβαίως, να έχει φυλάξει ο παραλήπτης κάπου το μήνυμα Μ και την υπογραφή s).

Τέλος, περιττό να αναφερθεί ότι όποτε το επιβάλλουν οι συνθήκες, μπορεί να κρυπτογραφήσει και ταυτόχρονα να υπογράψει μηνύματα. Μετά την παραπάνω ανάλυση έγινε κατανοητό πως ο αποστολέας του μηνύματος μπορεί να κάνει χρήση της ψηφιακής υπογραφής προκειμένου να πιστοποιήσει ένα έγγραφο στον παραλήπτη. Από την άλλη πλευρά όταν θέλει ο χρήστης να πιστοποιήσει το μήνυμα του ακολουθείται πάλι η ίδια διαδικασία. Είναι προφανές ότι η χρήση δεν έχει καμία σχέση με το όνομα του αποστολέα αλλά ούτε και με την υπογραφή του. Στην πραγματικότητα, είναι ένας μετασχηματισμός του μηνύματος όπου ενσωματώνει ένα μυστικό το οποίο γίνεται γνωστό μόνο στον αποστολέα. Κατά συνέπεια είναι άρρηκτα συνδεδεμένο και με τον αποστολέα, αλλά και με το μήνυμα το οποίο υπογράφει. Είναι επίσης προφανές ότι, σε αντίθεση με την χειρόγραφη υπογραφή, η ψηφιακή υπογραφή ενός υπογράφοντος θα είναι διαφορετική για κάθε μήνυμα (ψηφιακό έγγραφο) που υπογράφει. Οι ψηφιακές υπογραφές μπορούν να ανταποκριθούν στις λειτουργικές απαιτήσεις του νόμου εξίσου καλά με τις φυσικές υπογραφές, παρουσιάζουν όμως σε σχέση με αυτές σημαντικές διαφορές.

Κάπου εδώ πρέπει να αναφερθεί ότι κάθε ψηφιακή υπογραφή είναι μοναδική και συνοδεύει ένα και μόνο έγγραφο. Παρόλα αυτά μπορούν να ανταποκριθούν στις λειτουργικές απαιτήσεις του νόμου ακριβώς όπως οι χειρόγραφες υπογραφές παρουσιάζοντας όμως αρκετές διαφορές οι οποίες αναλύονται παρακάτω.

Κατ' αρχήν, η ψηφιακή δεν παρέχει σαφή μαρτυρία για την ταυτότητα του υπογράφοντος σε αντίθεση με την χειρόγραφη. Για να εξασφαλιστεί αυτό, απαιτείται επιπλέον πιστοποίηση, η οποία να συνδέει το κλειδί υπογραφής με τον ίδιο τον υπογράφοντα. Κάτι τέτοιο θα μπορούσε να αποδειχθεί με την επίκληση εξωτερικής πιστοποίησης, όπως ακριβώς συμβαίνει και με τις χειρόγραφες υπογραφές. Συνήθως όμως ο παραλήπτης ενός ψηφιακά υπογεγραμμένου εγγράφου επιθυμεί να είναι σε θέση να στηριχθεί στην υπογραφή χωρίς επιπλέον ελέγχους, γιατί κάτι τέτοιο θα ήταν αρκετά κουραστικό και θα χρειαζόταν επιπλέον χρόνο. Στο σημείο αυτό καλούνται οι Αρχές Πιστοποίησης, οι οποίες εκδίδουν τα ψηφιακά πιστοποιητικά, τα οποία πληροφορούν για την ταυτότητα του κατόχου και το δημόσιο κλειδί που χρησιμοποιείται, προκειμένου να επαληθευτεί η υπογραφή του σε κάποιο έγγραφο.

Έχει ασφαλώς προηγηθεί από την πλευρά της Αρχής Πιστοποίησης ο έλεγχος όλων εκείνων των στοιχείων που διασφαλίζουν την αυθεντικότητα της ταυτότητας του κατόχου του πιστοποιητικού, καθώς και ότι αυτός κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στο πιστοποιητικό.
Το πιστοποιητικό χρησιμοποιείται από τον παραλήπτη, προκειμένου αυτός να βεβαιωθεί για την ταυτότητα του υπογράφοντος.

Μια άλλη διαφορά είναι ότι στη διαδικασία της φυσικής υπογραφής, ο υπογράφων πρέπει να παρίσταται ο ίδιος και να έχει το προς υπογραφή έγγραφο

εμπρός του. Αντίθετα, στη περίπτωση της ψηφιακής υπογραφής υπάρχουν οι εξής δύο δυνατότητες:

- Το κλειδί υπογραφής βρίσκεται αποθηκευμένο στον υπολογιστή του υπογράφοντος και η υπογραφή τίθεται με την ενεργοποίηση κάποιας επιλογής σε ένα πρόγραμμα λογισμικού.
- Το κλειδί υπογραφής βρίσκεται αποθηκευμένο σε κάποια ειδική συσκευή (π.χ. Smart Card) η οποία πρέπει να είναι παρούσα και διαθέσιμη, ώστε το πρόγραμμα λογισμικού να επισυνάψει την υπογραφή.

Εύκολα γίνεται αντιληπτό πως κάποιος τρίτος μπορεί να χρησιμοποιήσει την ψηφιακή υπογραφή κάποιου άλλου. Στην ουσία μια ψηφιακή υπογραφή λέγεται ότι μπορεί να συγκριθεί με μια προτυπωμένη σφραγίδα όπου δηλώνεται το όνομα του αποστολέα. Γενικά για τη σωστή διακίνηση αρχείων δεν αρκεί μόνο ο αποστολέας να κάνει χρήση της ψηφιακής ταυτότητας αλλά και ο παραλήπτης να είναι σε θέση να διαπιστώσει αν η ψηφιακή υπογραφή που συνοδεύει αυτό το μήνυμα, που δέχεται, δεν είναι προϊόν από «παραχαράκτη» .

Επί πρόσθετα πρέπει να γίνει κατανοητό τι γίνεται στην περίπτωση όπου το άτομο Α επικοινωνεί με το άτομο Β σε πραγματικό χρόνο. Και πώς μπορεί ο Α να είναι βέβαιος ότι καθ' όλη τη διάρκεια της συνομιλίας τους θα μιλάει στον ίδιο το Β και όχι σε κάποιον άλλο; (ο Β θα μπορούσε να ήταν μια τράπεζα, ένα βιβλιοπωλείο on-line κ.λπ.). Αν το μήνυμα που έστελνε ο Β ήταν κάπως έτσι "Έλα Α, εγώ είμαι ο Β", τότε εύκολα διαπιστώνεται ότι τη στιγμή που έστειλε το μήνυμα, ήταν όντως εκείνος που το έγραφε. Εάν, όμως, ένας hacker κατορθώσει και υποκλέψει ολόκληρο το μήνυμα, καθώς και την υπογραφή, τότε θα μπορέσει να τα χρησιμοποιήσει αργότερα, για να υποδυθεί τον Β.

Το πρόβλημα, λοιπόν έγκειται ότι κάθε φορά που μιλάει ο παραλήπτης με τον αποστολέα, σε προκειμένη φάση ο Α με τον Β σε πραγματικό χρόνο, θέλει να είναι βέβαιος ότι μιλάει μαζί του και όχι με κάποιον hacker. Με άλλα λόγια, χρειάζεται έναν τρόπο επικύρωσης του χρήστη (user authentication), κάτι το οποίο δεν μπορεί να γίνει με απλή χρήση ψηφιακών υπογραφών.

Πριν αρχίσει ο Α να συνομιλεί σε πραγματικό χρόνο με τον Β, παράγει με χρήση ενός κατάλληλου προγράμματος έναν τυχαίο αριθμό (έστω ν) και του τον στέλνει. Στη συνέχεια, εκείνος δημιουργεί ένα μήνυμα που λέει κάτι σαν "Έλα Α, ο Β είμαι και μόλις μου έστειλες το ν, τι ακαταλαβίστικα πράγματα είναι αυτά;", το οποίο υπογράφει και του το στέλνει (το σημαντικό εδώ είναι να περιλαμβάνεται στο μήνυμα ο τυχαίος αριθμός ν). Όταν ο Α λάβει το μήνυμα με τον τυχαίο αριθμό που μόλις πριν παρήγαγε, μαζί με την ψηφιακή υπογραφή, είναι πλέον βέβαιος ότι μιλάει με τον Β και με κανέναν άλλο.

Ο τυχαίος αριθμός ν ονομάζεται πρόκληση (challenge). Η μη προβλεψιμότητά του σε συνδυασμό με μια ψηφιακή υπογραφή, παρέχει το ζητούμενο μηχανισμό επικύρωσης χρήστη. Βεβαίως, εννοείται ότι και ο Β μπορεί να χρησιμοποιήσει το μηχανισμό αυτό για να επικυρώσει την ταυτότητά του Α.

Το συμπέρασμα είναι πως ένα σύστημα κρυπτογράφησης και ψηφιακών υπογραφών, εξασφαλίζει σε μεγάλο βαθμό την ασφαλή διακίνηση μηνυμάτων.

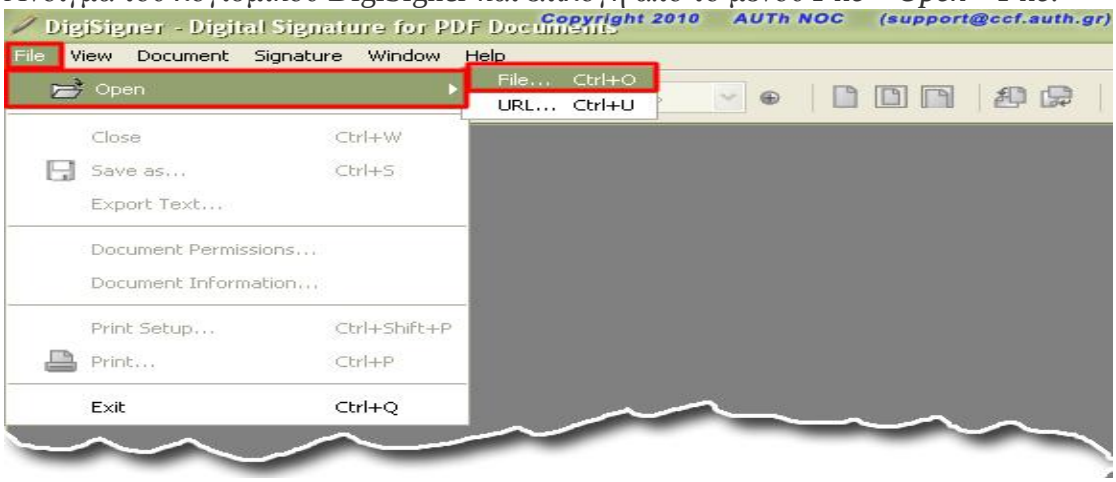
Κάτι τέτοιο όμως, δεν παρέχει όμως πλήρη προστασία απέναντι σε κάθε κακόβουλη προσπάθεια τρίτων

Παρακάτω αναλύεται ένα παράδειγμα με τη βοήθεια ενός προγράμματος για την προσθήκη μιας ψηφιακής υπογραφής το οποίο όμως προϋποθέτει τα εξής:

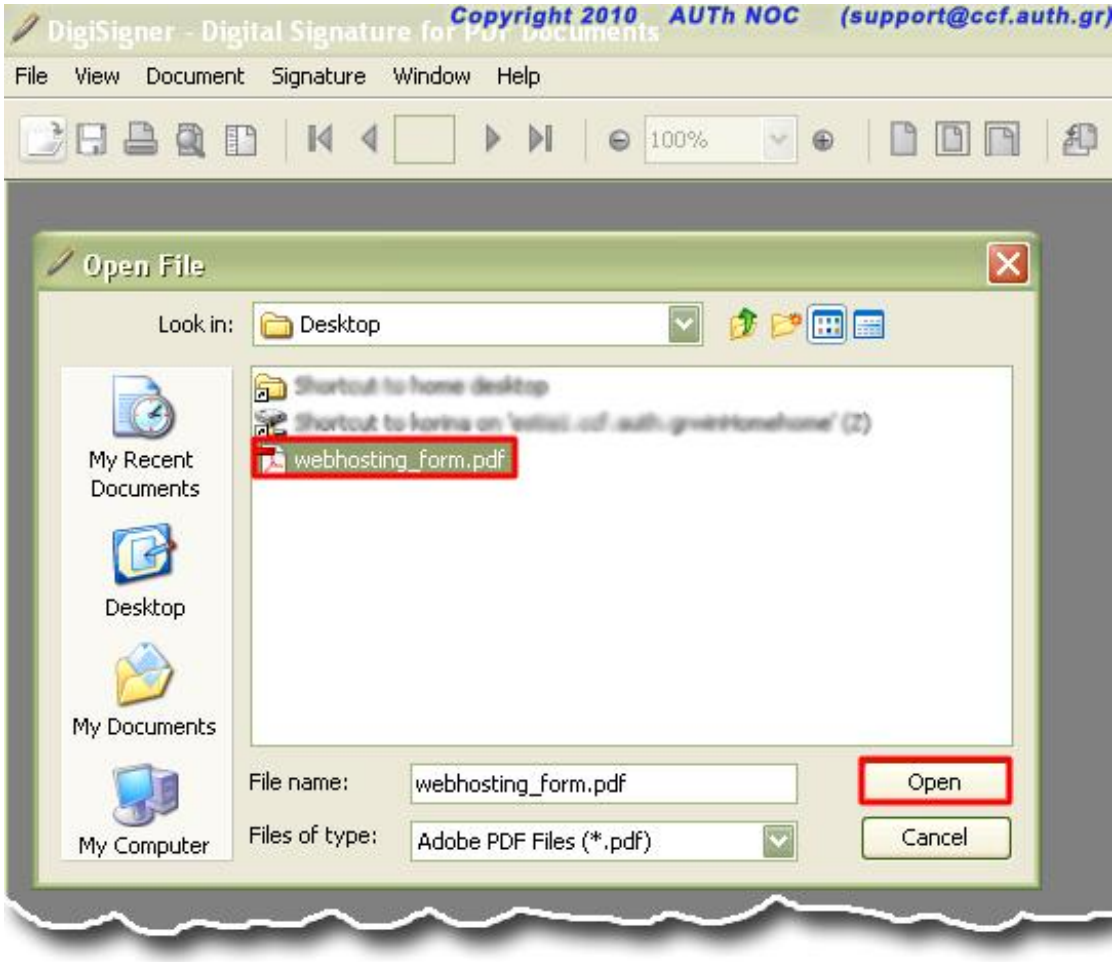
Ο χρήστης έχει στην κατοχή του ένα Ψηφιακό Πιστοποιητικό που έχει εκδοθεί από κάποια έγκυρη Αρχή Πιστοποίησης όπως είναι η Αρχή Πιστοποίησης (ΑΠ) . Υπάρχει στον υπολογιστή του εγκατεστημένο κατάλληλο λογισμικό που έχει τη δυνατότητα να προσθέτει την ψηφιακή του υπογραφή σε έγγραφο. Ένα τέτοιο λογισμικό που διατίθεται δωρεάν είναι το DigiSigner το οποίο κατά την εγκατάστασή του στον υπολογιστή δεν απαιτεί καμία επιπλέον ρύθμιση.

Ρυθμίσεις

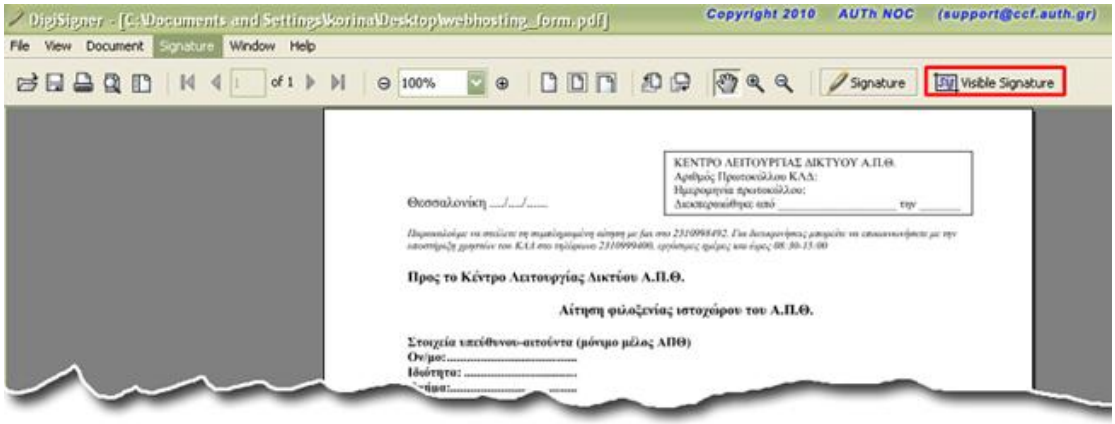
Άνοιγμα του λογισμικού DigiSigner και επιλογή από το μενού *File->Open->File*.



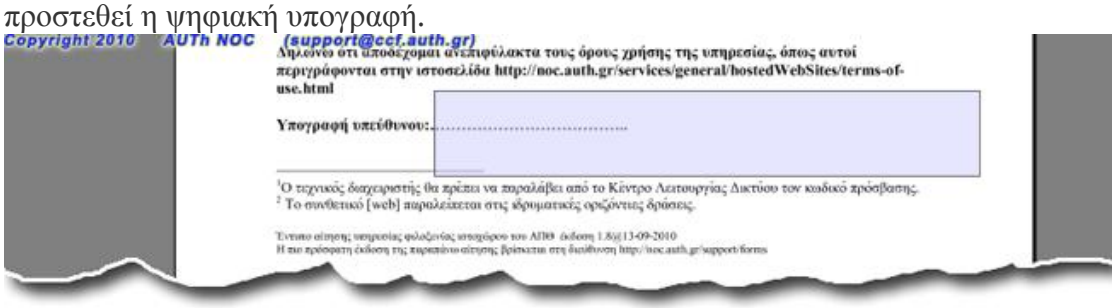
Αναζήτηση του αρχείου pdf που επιθυμεί ο χρήστης να υπογράψει ψηφιακά και επιλογή *Open*..



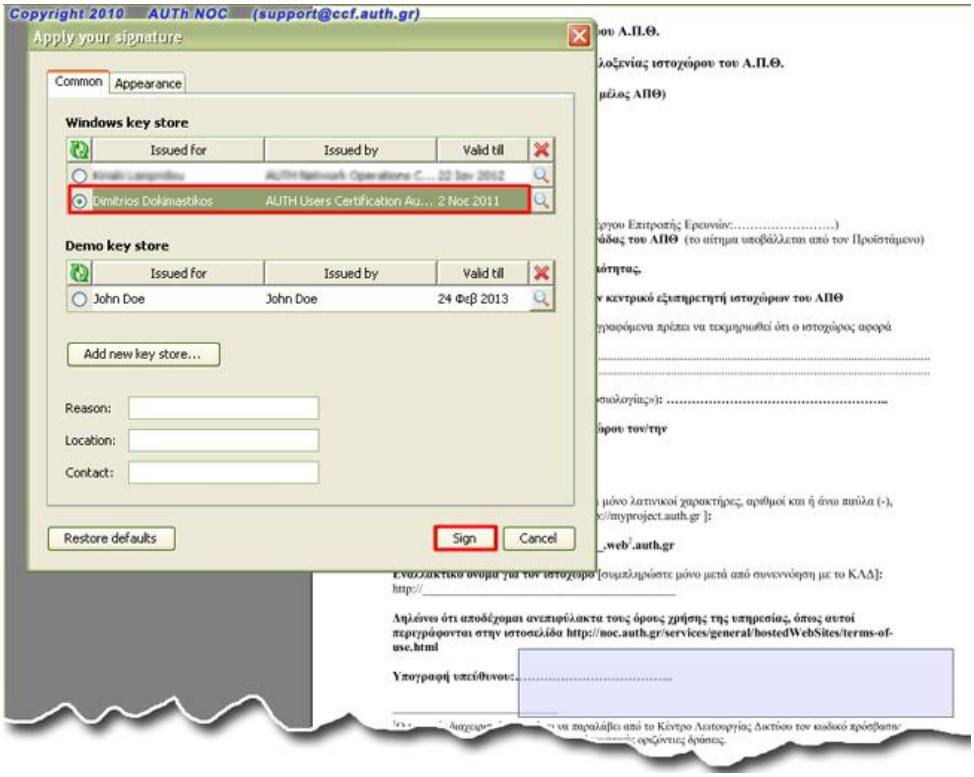
Μόλις ανοίξει το έγγραφο και επιλογή από το μενού *Visible Signature*.



Το βέλος του ποντικιού γίνεται σταυρός. Πρέπει να επιλεχθεί η περιοχή όπου θα προστεθεί η ψηφιακή υπογραφή.

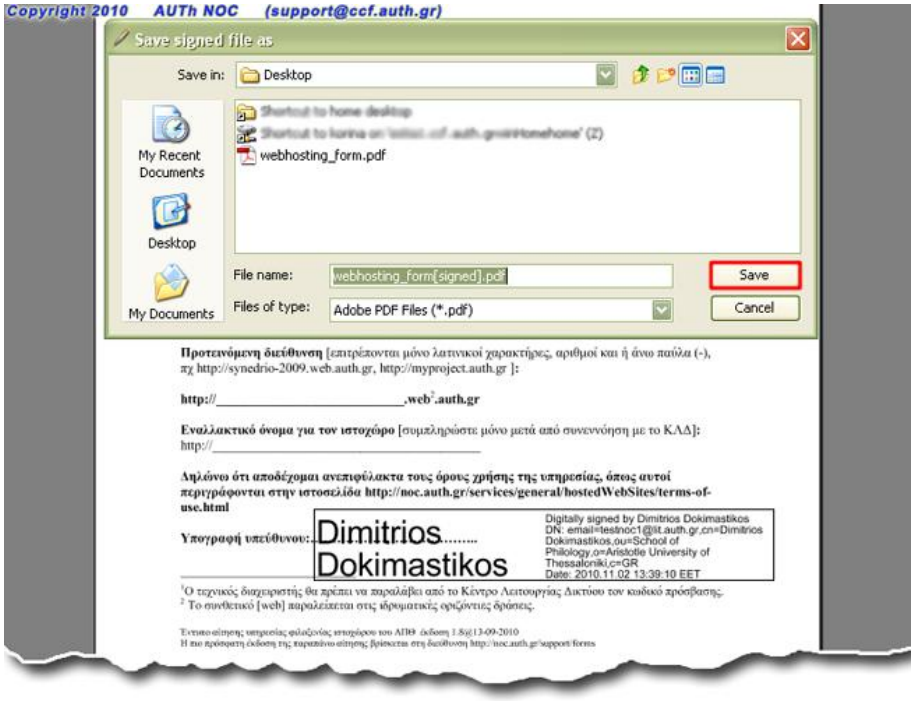


Στο παράθυρο που ανοίγει πρέπει να γίνει επιλογή του ψηφιακού πιστοποιητικού και στη συνέχεια *Sign*.



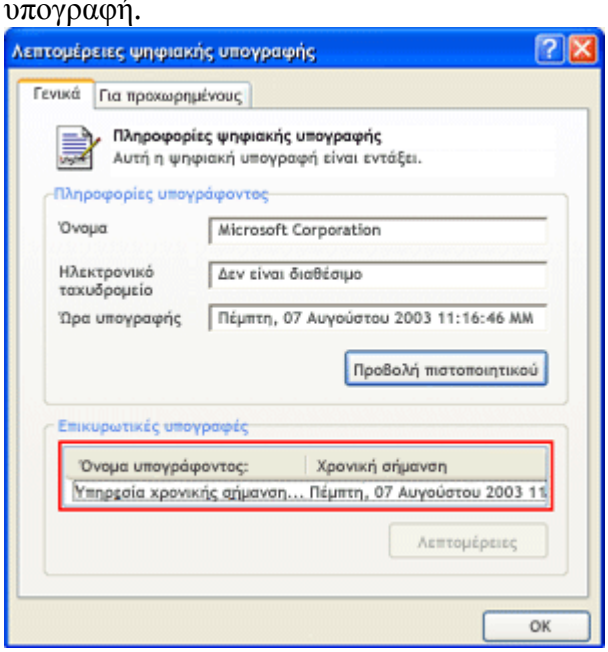
Στο σημείο αυτό και μόνο στην περίπτωση που χρησιμοποιεί κρυπτογραφική συσκευή (eToken, eKey) για το πιστοποιητικό του θα του ζητηθεί ο κωδικός προστασίας του.

Μέσα σε λίγα δευτερόλεπτα θα εμφανιστεί η ψηφιακή υπογραφή στο έγγραφο.
Επιλογή από το μενού *File->Save As* και αποθήκευση του εγγράφου με το όνομα που επιθυμεί.

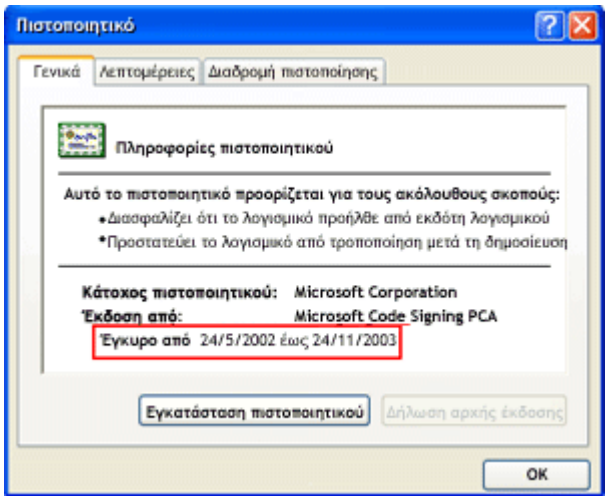


Πότε μια ψηφιακή υπογραφή είναι αξιόπιστη;

Το παράθυρο διαλόγου **Λεπτομέρειες της Ψηφιακής υπογραφής** εμφανίζει ένα μήνυμα στο επάνω μέρος του παραθύρου αυτού και το οποίο επιβεβαιώνει ότι η ψηφιακή υπογραφή είναι εντάξει. Επιπλέον οι λεπτομέρειες της χρονικής σήμανσης **Υπογραφές Ανταπόκρισης** υποδεικνύουν ότι η αρχή έκδοσης του πιστοποιητικού, στο συγκεκριμένο παράδειγμα η Verisign, έχει επαληθεύσει και εγκρίνει την ψηφιακή υπογραφή.



Τα δεδομένα για την χρονική σήμανση θα πρέπει να είναι όντος της περιοχής των ημερομηνιών **Έγκυρο από** στο πιστοποιητικό. Για να εμφανιστεί η περιοχή των ημερομηνιών κάντε κλικ στην καρτέλα **Προβολή πιστοποιητικού.**



Ο εκδότης — στο συγκεκριμένο παράδειγμα, η Microsoft Corporation — θα πρέπει να είναι αξιόπιστος εκδότης από προεπιλογή στους υπολογιστές που εκτελούν το λειτουργικό σύστημα Microsoft Windows. Τα πιστοποιητικά για τη Microsoft βρίσκονται στο χώρο αποθήκευσης των αξιόπιστων κεντρικών αρχών έκδοσης πιστοποιητικών. Εάν ο εκδότης δεν είναι αξιόπιστος από προεπιλογή, θα πρέπει να χαρακτηρίσει ρητά το συγκεκριμένο εκδότη ως αξιόπιστο. Αλλιώς, το περιεχόμενο που υπογράφεται από αυτόν τον εκδότη δεν περνά από τους ελέγχους ασφαλείας λογισμικού.

Τι πρέπει να κάνει κάποιος αν υπάρξει πρόβλημα με την υπογραφή

Όταν υπάρχει πρόβλημα με κάποια ψηφιακή υπογραφή, τότε ανάλογα με την περίπτωση υπάρχουν οι παρακάτω λύσεις:

- Επικοινωνία με την πηγή του υπογεγραμμένου περιεχομένου για την ενημέρωση τους ότι υπάρχει κάποιο πρόβλημα με την υπογραφή.
- Επικοινωνία με τον υπεύθυνο διαχειριστή για την υποδομή ασφαλείας της εταιρείας.
- Εάν η μακροεντολή ή άλλο ενεργό περιεχόμενο που σχετίζεται με το έγγραφο είναι αξιόπιστο, μπορεί να γίνει αποθήκευση του εγγράφου σε μια αξιόπιστη θέση. Τα έγγραφα σε αξιόπιστες θέσεις επιτρέπεται να εκτελούνται χωρίς να ελέγχονται από το σύστημα ασφαλείας του Κέντρου αξιοπιστίας. Η χρήση αξιόπιστων θέσεων είναι καλύτερη επιλογή από το να κατεβάσετε τις ρυθμίσεις επιπέδου ασφαλείας για όλες τις μακροεντολές.

2.2 Ηλεκτρονικές συναλλαγές μέσω ηλεκτρονικού καταστήματος

Στις μέρες μας θα πρέπει να δίνεται ιδιαίτερη έμφαση στο θέμα της ασφάλειας των συναλλαγών καθώς σε μια ηλεκτρονική επικοινωνία είναι ιδιαίτερα χρήσιμη η εμπιστοσύνη μεταξύ των μερών που συνδιαλέγονται. Για παράδειγμα ένα ηλεκτρονικό κατάστημα αν θέλει να φροντίζει για την ασφάλεια των πελατών του θα πρέπει να πληροί όλα τα συστήματα ασφαλείας καθώς και να παρέχει πληροφορίες για την πιστοποίηση της ταυτότητας του.

Κάποια από τα συστήματα ασφαλείας που θα πρέπει να χρησιμοποιεί ώστε να διασφαλίζει την ασφάλεια των συναλλαγών των πελατών του είναι τα εξής :

- Digital ID δηλαδή ένα ψηφιακό ταυτότητας από κάποιο αναγνωρισμένο φορέα πιστοποίησης ώστε να μπορεί να επιβεβαιώνει την ταυτότητα του εμπόρου που πραγματοποιεί την αγορά.
- Ένα πρωτόκολλο ασφαλείας (Secure electronic Transaction).
- Μια ασφαλή σύνδεση.

Ένα ηλεκτρονικό κατάστημα θα πρέπει να παρέχει συνεχείς ελέγχους ώστε να μπορεί να διασφαλίζει εγκυρότητα και ασφάλεια στους πελάτες του και αυτοί οι έλεγχοι θα πρέπει να γίνονται ανεξάρτητα από το αν η πρόσβαση στο διαδίκτυο είναι από τον υπολογιστή ή από κινητό τηλέφωνο. Γι αυτό οι ιδιοκτήτες θα πρέπει να ζητούν συνεχή ενημέρωση από τους ειδικούς για όλες τις δυνατές λύσεις.

Τέλος όσον αφορά την ταυτότητα του ηλεκτρονικού καταστήματος θα πρέπει να παρουσιάζει με ακριβή στοιχεία σε όποιον την ζητήσει, να μπορεί να παρέχει με ειλικρίνεια ποιος είναι ο πραγματικός ιδιοκτήτης του καταστήματος.

Συγκεντρωτικά κάποιες από τις πληροφορίες που θα πρέπει να παρουσιάζει ένα ηλεκτρονικό κατάστημα είναι οι εξής :

- Μέθοδος αποστολής και πληρωμής.
- Χρόνος παράδοσης του προϊόντος.
- Επιβεβαίωση της παραγγελίας.
- Πραγματική ταυτότητα του ιδιοκτήτη του καταστήματος
- Τυχόν αλλαγές ή και επιστροφές και τρόπος ακύρωσης της παραγγελίας
- Τελική τιμή του προϊόντος, να συμπεριλαμβάνεται και το ΦΠΑ και οι οποιοιδήποτε φόροι αλλά και κόστος μεταφοράς αν φυσικά υπάρχει.
- Εγγύηση του προϊόντος.

2.3 Ηλεκτρονικές Πληρωμές

Με την συνεχή εξέλιξη της τεχνολογίας αλλά και του internet πολλές επιχειρήσεις με σκοπό να διευκολύνουν την πρόσβαση των πελατών τους αλλά και για να αυξήσουν το πελατολόγιο τους με άλλους που είναι πιο οικείοι με την τεχνολογία, έχουν οδηγηθεί στην πραγματοποίηση συστήματα και μεθόδων και ηλεκτρονικών πληρωμών. Αυτό έχει σαν αποτέλεσμα την υποστήριξη του ηλεκτρονικού εμπορίου αλλά και την ανάπτυξη στο σύγχρονο επιχειρησιακό περιβάλλον.

Τα παλιότερα χρόνια όταν δεν είχε εξαπλωθεί η έννοια των ηλεκτρονικών πληρωμών η διαδικασία γινόταν με την καταβολή ενός ποσού στην τράπεζα. Όμως αυτός ο τρόπος σιγά άρχιζε να μην συμβαδίζει με τους γρήγορους ρυθμούς ανάπτυξης και τις σύγχρονες διαδικτυακές συναλλαγές. Έτσι για τον λόγο αυτό μια σειρά από συστήματα ηλεκτρονικών πληρωμών αναπτύχθηκε σταδιακά.

Οι ηλεκτρονικές πληρωμές αποτελούν αναπόσπαστο κομμάτι του ηλεκτρονικού εμπορίου. Γενικά θα λέγαμε ότι περιλαμβάνει οποιαδήποτε μορφή πληρωμής από τις επιχειρήσεις, τις τράπεζες ή τις δημόσιες υπηρεσίες από πολίτες ή επιχειρήσεις οι οποίες γίνονται μέσω του ηλεκτρονικού δικτύου.

Κάποιες κατηγορίες ηλεκτρονικών πληρωμών μπορούν να ταξινομηθούν σύμφωνα με τις συναλλαγές που χρησιμοποιούν:

- Μέσω διαδικτύου. Είναι η πιο σύγχρονη μορφή πληρωμών καθώς έχει εύκολη πρόσβαση στο διαδίκτυο και η πλειοψηφία των καταναλωτών το χρησιμοποιεί. Αυτό έχει σαν αποτέλεσμα να καθιστά τα συστήματα των ηλεκτρονικών πληρωμών ιδιαίτερα σημαντικά για την ανάπτυξη του ηλεκτρονικού εμπορίου.
- Μέσω τηλεφώνου. Αυτή η κατηγορία πληρωμής μέσω τηλεφωνικού δικτύου είναι μια καινούργια μορφή πληρωμής. Στόχος είναι να εκμεταλλευτούν οι επιχειρήσεις και όχι μόνο αυτή την σύγχρονη ανάπτυξη της τεχνολογικής υποδομής αλλά και την διείσδυση του τηλεφώνου στις ηλεκτρονικές συναλλαγές.
- Μέσω κινητής τηλεφωνίας(m-payments). Το WAP επιτρέπει την εκτέλεση βασικών χρηματικών συναλλαγών οπουδήποτε και αν βρίσκεσαι ανεξαρτήτως χρόνου και τόπου από κινητές και ασύρματες συσκευές. Για το λόγο αυτό επειδή είναι πιο αυτόνομο έχει ευρεία αποδοχή και η χρήση του από το καταναλωτικό κοινό το κάνει ακόμα πιο δημοφιλές στο ηλεκτρονικό εμπόριο.

Σε μια ηλεκτρονική συναλλαγή για να γίνει αποδέκτη θα πρέπει να έχουν πρόσβαση τόσο ο πελάτης όσο και ο έμπορος αλλά και οι δυο επίσης να έχουν έναν τραπεζικό λογαριασμό σε κάποια τράπεζα ή χρηματοπιστωτικό οργανισμό.

Μια συναλλαγή μπορεί να έχει τα παρακάτω βήματα:

- Ο πελάτης στην αρχή βρίσκει το site που τον ενδιαφέρει με την προϋπόθεση να διαλέξει τα κατάλληλα προϊόντα για εκείνον. Για να κλείσει η συναλλαγή ο πελάτης θα πρέπει να διαλέξει τον τρόπο πληρωμής που επιθυμεί. Δηλαδή αν θέλει να πληρώσει με πιστωτική κάρτα στέλνει στο site και κατ' επέκταση στον έμπορο τον αριθμό της πιστωτικής κάρτας και όποιες άλλες πληροφορίες χρειάζεται.
- Στη συνέχεια ο έμπορος προωθεί αυτές τις πληροφορίες για να εξακριβώσει την εγκυρότητα του τρόπου πληρωμής.
- Με την σειρά της βέβαια η τράπεζα παρέχει στον πελάτη μια απόδειξη πληρωμής για να έχει και εκείνος μια απόδειξη από την συναλλαγή.
- Από την άλλη πλευρά επίσης η τράπεζα του εμπόρου τον ενημερώνει πως η συναλλαγή ειναι έγκυρη και πως έχει χρεωθεί το απαραίτητο ποσό του προϊόντος και μπορεί να προχωρήσει η διαδικασία για την παράδοση του.
- Τέλος, ο έμπορος στέλνει όλες τις συμφωνημένες υπηρεσίες στον πελάτη.

2.4 Πιστωτικές Κάρτες

Ίσως από τα πρώτα χρόνια που εμφανίστηκε το ηλεκτρονικό εμπόριο ένας από τους βασικούς τρόπους αγοράς ήταν αυτός μέσω πιστωτικών καρτών. Η αποστολή του αριθμού γινόταν μέσω ηλεκτρονικού ταχυδρομείου ή fax. Κάτι τέτοιο όμως δεν ήταν καθόλου εύχρηστο για τους εμπόρους καθότι θα έπρεπε πριν στείλουν τις παραγγελίες να ελέγξουν στις τράπεζες που είχαν εκδώσει τις πιστωτικές κάρτες, τα προσωπικά δεδομένα των πελατών. Ο τρόπος αυτός απαιτούσε αρκετό χρόνο και

δεν παρείχε ασφάλεια. Με τη βοήθεια λοιπόν των on-line ψηφιακών συναλλαγών η εξακρίβωση στοιχείων και η χρέωση της πιστωτικής κάρτας του καταναλωτή γίνεται απευθείας χωρίς χρονοβόρες διαδικασίες και πιθανά λάθη. Ο πελάτης δίνει τα προσωπικά του στοιχεία, τη διεύθυνση που επιθυμεί να αποσταλούν τα προϊόντα και τα στοιχεία της πιστωτικής του κάρτας. Τα δεδομένα αυτά μεταφέρονται με ασφάλεια από τον Web browser του καταναλωτή με τη χρήση πρωτοκόλλων κρυπτογράφησης (όπως είναι το SSL ή το SET τα οποία και θα αναλύσουμε παρακάτω).Ο έμπορος επιβεβαιώνει τα στοιχεία του πελάτη, η παραγγελία θεωρείται ολοκληρωμένη και ο έμπορος την στέλνει στον πελάτη.

Οι πιστωτικές κάρες είναι από τις πλέον γνωστές και διαδεδομένες μεθόδους στις ηλεκτρονικές διεθνείς συναλλαγές. Ωστόσο η χρήση τους δεν διαφέρει πολύ από τις φυσικές συναλλαγές. Στις φυσικές συναλλαγές ο πελάτης δίνει την κάρτα του στον έμπορο χέρι με χέρι για να την χρεώσει, ενώ στις ηλεκτρονικές συναλλαγές ο πελάτης δίνει τις πληροφορίες της κάρτας στον έμπορο για να την χρεώσει μέσω του διαδικτύου. Κατά την πληρωμή μέσω πιστωτικών καρτών στο διαδίκτυο ο πελάτης θα πρέπει να δώσει τις πληροφορίες της κάρτας του, τον αριθμό της πιστωτικής αλλά και όποιες άλλες πληροφορίες μπορεί να χρηστούν όπως ημερομηνία λήξης της κάρτας κ.α. στην συνέχεια ο έμπορος ζητά από την τράπεζα του να επιβεβαιώσει αυτά τα στοιχεία ώστε να προχωρήσει ή όχι η παραγγελία. Στην περίπτωση της έγκρισης ειδοποιείται ο έμπορος με σκοπό να στείλει την παραγγελία στον πελάτη. Η τράπεζα του πελάτη με την σειρά της προωθεί τα χρήματα στον λογαριασμό του εμπόρου μέσω ενός διατραπεζικού συστήματος. Αυτός ο τρόπος πληρωμής παρέχει άμεση πρόσβαση στους τραπεζικούς λογαριασμούς τόσο του αγοραστή όσο και του πωλητή και καταγράφει τις κινήσεις των μεταβολών και των δυο.

Είναι ευρέως γνωστό ότι με την εμφάνιση των ηλεκτρονικών συναλλαγών αλλά και του ηλεκτρονικού εμπορίου οι απάτες μέσω των πιστωτικών καρτών έχουν αυξηθεί. Γι αυτό τον λόγο για να γίνει η έγκριση απαιτείται αυστηρή ασφάλεια μεταξύ των συναλλαγών και είναι σημαντικό οι αριθμοί των πιστωτικών καρτών να είναι δυσανάγνωστες εκτός από τον πελάτη και την τράπεζα του. Με τον όρο δυσανάγνωστα εννοείται ότι στέλνονται με μορφή κρυπτογράφησης ή κρυπτογραφικού μηνύματος καθώς υπάρχει περίπτωση το μήνυμα να υποκλαπεί.

Όλες οι πληροφορίες που συμπεριλαμβάνουν και τα προσωπικά δεδομένα κρυπτογραφούνται και διατηρούνται εμπιστευτικές. Αυτό σημαίνει ότι οι πληροφορίες ανταλλάσσονται μεταξύ του πελάτη και της επιχείρησης ή εταιρείας και ότι κανένας άλλος δεν μπορεί να έχει πρόσβαση σε αυτά τα δεδομένα. Το SSL είναι το πιο γνωστό και σύνηθες επίπεδο ασφαλειών.

Το πρωτόκολλο SSL παρέχει TCP/IP ασφάλεια σύνδεσης η οποία με την σειρά της έχει 3 βασικές ιδιότητες.

- Προστατεύει την ακεραιότητα των δεδομένων που μεταδίδονται κατά την διάρκεια μιας συναλλαγής αλλά και τα μηνύματα αυθεντικοποιούνται και ελέγχονται ως προς την ακεραιότητα τους κατά την μετάδοση.
- Εφόσον η σύνδεση κρυπτογραφείται με αυτόν τον τρόπο επιτυγχάνεται και η εμπιστευτικότητα των δεδομένων που μεταδόθηκαν κατά την συναλλαγή.
- Με την κρυπτογράφηση δημόσιου κλειδιού οι επικοινωνούντες μπορούν να ταυτοποιούν ο ένας τον άλλον αμοιβαία και άμεσα.

2.5 Ηλεκτρονικό εμπόριο και ηλεκτρονική δημοπρασία

Το μέλλον του εμπορίου πλέον κρίνεται από το internet. Στις μέρες μας το μέλλον βρίσκεται στην έννοια της ηλεκτρονικής επιχείρησης αφού είναι γεγονός ότι υπάρχει μια ραγδαία τεχνολογική πρόοδος στον τομέα των δικτυακών υποδομών. Ειδικά στην Ελλάδα, η αύξηση των χρηστών του διαδικτύου την προηγούμενη δεκαετία είναι κατακόρυφη: από ένα εκατομμύριο χρήστες το 2000 άγγιξε τα 4 εκατομμύρια χρήστες το 2010 και φυσικά αυτός είναι ένας αριθμός που ολοένα αυξάνεται.

Φυσικά, ο προβληματισμός γύρω από την ασφάλεια ενός on line καταστήματος από τον εκάστοτε πελάτη είναι μεγάλος κυρίως όσον αφορά την ασφάλεια των πληρωμών μέσω Διαδικτύου. Την ανησυχία αυτή τη μοιράζονται τόσο οι επιχειρηματίες όσο και οι πελάτες. Η πιο συνηθισμένη μέθοδος πληρωμής είναι με χρέωση πιστωτικής κάρτας όπου πολλές φορές δεν θεωρείται και από τους πιο ασφαλείς τρόπους. Για αυτό ήταν σκόπιμο να εφευρεθούν και άλλες μέθοδοι, όπως με την έκδοση ηλεκτρονικού «χρήματος» που πιστώνεται σε ένα λογαριασμό αλλά δεν συνδέεται άμεσα με τον τραπεζικό σας λογαριασμό.
Η πιο γνωστή εταιρία τέτοιου τύπου είναι η pay-pal, που επιτρέπει στο χρήστη να διαχειρίζεται ένα λογαριασμό περιορισμένου υπολοίπου και μέσα από αυτόν να πραγματοποιεί τις συναλλαγές του. Ωστόσο στην Ελλάδα η χρέωση πιστωτικής κάρτας αποτελεί προς το παρόν την κύρια μέθοδο πραγματοποίησης πληρωμών μέσω Διαδικτύου.

Ηλεκτρονική δημοπρασία

Τα τελευταία χρόνια ολοένα και αυξάνονται οι άνθρωποι που χρησιμοποιούν την ηλεκτρονική δημοπρασία προκειμένου να αποκτήσουν ένα αντικείμενο ή να το πουλήσουν. Τα αντικείμενα που πωλούνται στις δημοπρασίες αυτές ποικίλλουν καθώς και οι τιμές επίσης. Η ηλεκτρονική δημοπρασία συνήθως διαρκεί αρκετές ημέρες και οι τιμές που μπορεί να πετύχει κανείς είναι συχνά πολύ πιο χαμηλές από αυτές του εμπορίου. Πρέπει όμως να σημειωθεί πως συχνά η ανωνυμία και η αδυναμία των χρηστών να ελέγξουν το προϊόν έχει ως αποτέλεσμα τον κίνδυνο εξαπάτησης των αγοραστών και γι αυτό και σε αυτή την περίπτωση κρίνεται αναγκαία η χρήση της κρυπτογράφησης.

Ψηφιακά συστήματα πληρωμής (e-payment)

Όπως ειπώθηκε και παραπάνω, ο παραδοσιακός τρόπος πληρωμής δεν ήταν αρκετός για τις ηλεκτρονικές συναλλαγές εφόσον όλα εξελίσσονται διαδικτυακά. Έτσι, στην αγορά εμφανίστηκαν καινούριοι μέθοδοι πληρωμής και διακίνησης χρημάτων. Για αυτό και η ηλεκτρονική μεταφορά χρημάτων είναι ένα ζήτημα που εξελίσσεται συνεχώς. Η πιο γνωστή μέθοδος πληρωμής για αγορές μέσω διαδικτύου είναι οι πιστωτικές κάρτες. Παρόλα αυτά, πολλοί χρήστες είναι ακόμα διστακτικοί σε τέτοιου είδους συναλλαγές κυρίως λόγω έλλειψης ασφάλειας. Σύμφωνα με τον κατασκευαστή ηλεκτρονικών καταστημάτων, αρκετά από τα συστήματα ηλεκτρονικής πληρωμής αποτελούνται από σύνθετα πακέτα λογισμικού που εφαρμόζονται για τις ψηφιακές συναλλαγές πραγματικού χρόνου.

2.6 Smart Cards

Κρυπτογράφηση όμως παρατηρείται όμως και στις έξυπνες κάρτες(smart cards) οι οποίες ότι αποτελούν την εξέλιξη των καρτών μαγνητικής λωρίδας. Οι συγκεκριμένες κάρτες είναι σχεδιασμένες έτσι ώστε να μπορούν να αποθηκεύουν έναν μεγάλο όγκο πληροφοριών παρέχοντας ταυτόχρονα τη δυνατότητα κρυπτογράφησης και χειρισμού ηλεκτρονικών υπογραφών για την ασφάλεια τους.

Η ιδέα της παρουσιάστηκε για πρώτη φορά στη Γαλλία το 1974 αλλά παρουσιάστηκε στο κοινό το 1981. Στις μέρες μας το πρόβλημα εντοπίζεται στο ότι πολλοί θεωρούν πως αυτές οι κάρτες είναι πιστωτικές ή τραπεζικές και αυτός είναι και ο λόγος που δεν αναγνωρίζεται το εύρος των δυνατοτήτων τους στους τομείς του εμπορίου, της βιομηχανίας αλλά και της δημόσιας διοίκησης.

2.7 E-banking

Σε πρακτική βάση, η τράπεζα προσπαθεί να επιβάλλει μια σειρά πρόσθετων μηχανισμών και ασφαλείας οι οποίοι δεν υπάρχουν στην περίπτωση των πιστωτικών καρτών κάτι που σημαίνει πως το σύστημα ουσιαστικά είναι απαραβίαστο αν φυσικά η χρήση των μηχανισμών αυτών είναι σωστή από την πλευρά του πελάτη. Παράδειγμα στην περίπτωση αυτή θεωρείται η χρήση λίστας κωδικών TAN ή διαφορετικά Transaction Authorization Numbers – Αριθμοί Εξουσιοδότησης Συναλλαγής.

Εντούτοις, αν κάποιος πελάτης κατά λάθος καταστεί θύμα απάτης από διαδικτυακούς τόπους παραποίησης ταυτότητας, δηλαδή να δώσει τα στοιχεία του σε κόμβο που προσποιείται ότι είναι αυτός της τράπεζας, τότε η ίδια η τράπεζα αναφέρει σε σχετικό έγγραφο ότι εφόσον έχει ενημερώσει εξαρχής τον πελάτη της σχετικά και αυτός έκανε κάτι εκτός του δικού της δικτύου, δεν φέρει καμία απολύτως ευθύνη. Στην περίπτωση αυτή εδώ βέβαια δεν ισχύει η αρχή της απόδειξης της μη-εντιμότητας όπως για τις ηλεκτρονικές πιστωτικές κάρτες.

Στους όρους χρήσης μάλιστα της λίστας κωδικών TAN μιας γνωστής τράπεζας αναφέρεται ρητά ότι : "...Κανένας άλλος δεν πρέπει να γνωρίζει τους αριθμούς TAN. Η τράπεζα δεν φέρει καμία ευθύνη, για συναλλαγές που έγιναν από άλλο πρόσωπο, παρά τη θέλησή σας, σε περίπτωση απώλειας ή διαρροής αριθμών TAN...’’

Με διαφορετικά λόγια, η τράπεζα καλύπτει το δικό της μερίδιο με αποκλειστική δική της ευθύνη με την προσφορά αυτού του πρόσθετου και υποχρεωτικού μέτρου ασφάλειας καθώς έγκειται στον ίδιο τον χρήστη να διαφυλάξει την σωστή εφαρμογή του όρου.

Θα πρέπει πάντως να αναφερθεί πως στις μέρες μας το επίπεδο κατάρτισης του προσωπικού των τραπεζών και της ενημέρωσης των πελατών τους σχετικά με την διάθεση και χρήση των νέων συσκευών παραγωγής κωδικών TAN μιας χρήσης, θεωρείται τουλάχιστον επιεικώς απαράδεκτο. Για παράδειγμα, η προμήθεια των αντίστοιχων συσκευών TAN χρεώνεται στον κάθε πελάτη ως πρόσθετη προαιρετική υπηρεσία όπως φυσικά και οι πιστωτικές κάρτες και χωρίς όμως να παρέχεται μαζί ένα αναλυτικό εγχειρίδιο οδηγιών, ούτε επίσης οι αναλυτικές τεχνικές προδιαγραφές και τέλος ούτε καν οι αναλυτικοί όροι χρήσης όπου καθορίζονται τα όρια ευθύνης του κάθε μέρους της τράπεζας και του πελάτη αντίστοιχα.

Το γεγονός αυτό μπορεί να οφείλεται βέβαια στο ότι η διάδοση και η χρήση κάποιων παρόμοιων διαδικασιών στις ηλεκτρονικές τραπεζικές συναλλαγές είναι ακόμη σε πολύ πρώιμο στάδιο στην Ελλάδα, κάτι που έχει ως αποτέλεσμα το αντίστοιχο ενδιαφέρον να είναι περιορισμένο, τόσο από την πλευρά των πελατών οι οποίοι συνήθως δεν επιδιώκουν περαιτέρω ενημέρωση, όσο και από την ίδια την τράπεζα η οποία δεν θέλει να επωμιστεί το βάρος και το κόστος της "εκπαίδευσης" των πελατών σε αυτά τα νέα συστήματα και δεδομένα.

Είναι γεγονός πως προηγμένη τεχνολογία για την πλήρη εξασφάλιση των ηλεκτρονικών συναλλαγών μέσω του e-Banking υπάρχει πραγματικά. Τα σημερινά συστήματα κρυπτασφάλισης θεωρούνται τόσο ασφαλή και παράλληλα τόσο προσιτά στην καθημερινή χρήση τους, ώστε λίγοι μπορούν να συνειδητοποιήσουν τι ακριβώς συμβαίνει όταν κάποιος προσπαθεί μα χρησιμοποιήσει μια ηλεκτρονική τραπεζική κάρτα σε ένα μηχάνημα αυτόματης ανάληψης χρημάτων ή διαφορετικά ATM. Ωστόσο, υπάρχει σοβαρή έλλειψη τεχνογνωσίας και πρωτίστως εκπαίδευσης του αρμόδιου προσωπικού των τραπεζικών εταιριών στα αντίστοιχα θέματα, που έχει ως αποτέλεσμα η όλη διαδικασία να μετατρέπεται σε εξαιρετικά δύσκολη και δυσνόητη για τους ενδιαφερόμενους πελάτες και οι οποίοι κατά κανόνα είναι λιγότερο ειδικοί επί των θεμάτων ασφαλούς χρήσης των υπηρεσιών ηλεκτρονικών συναλλαγών και e-Banking.

Η εξάπλωση του e-banking αποτελεί γεγονός πως είναι ραγδαία σε όλο τον κόσμο. Οι ειδικοί εκτιμούν ότι στο μέλλον οι σύγχρονες εμπορικές τράπεζες θα δραστηριοποιούνται αποκλειστικά μέσω των νέων ηλεκτρονικών τεχνολογιών. Ενδεικτικά αναφέρεται πως στη Γερμανία το 42% του πληθυσμού χρησιμοποιεί τις υπηρεσίες e-banking, στη Σουηδία το 28%, στη Βρετανία το 7%. Οι πελάτες, είτε ιδιώτες είτε επιχειρήσεις, ωφελούνται σημαντικά από τη χρήση των υπηρεσιών e-banking καθώς τους παρέχεται η δυνατότητα να διεκπεραιώνουν καθημερινά ένα μεγάλο μέρος των ηλεκτρονικών συναλλαγών τους με την τράπεζα ευκολότερα, γρήγορα και με ασφάλεια 24 ώρες το 24ωρο, 365 μέρες το χρόνο. Για τις επιχειρήσεις το όφελος θεωρείται ακόμη μεγαλύτερο, καθώς περιορίζεται το κόστος λειτουργίας τους όσον αφορά σε λειτουργικά έξοδα, προμήθειες και κινδύνους απώλειας χρήματος ενώ παράλληλα εξοικονομείται πολύτιμος χρόνος για άλλες εργασίες.

Η ταυτοποίηση του χρήστη ενός συστήματος είναι η αναγνώριση της ταυτότητάς του από το σύστημα, ώστε να διασφαλίζεται ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε αυτό.

(α) Ταυτοποίηση χρήστη κατά την είσοδο στην υπηρεσία

Η είσοδος στην υπηρεσία eBanking επιτυγχάνεται με τη συνδυασμένη χρήση των προσωπικών κωδικών σας: Όνομα Χρήστη (user name) και Κωδικός Πρόσβασης (PIN). Οι κωδικοί αυτοί σας παραδίδονται κατά την εγγραφή σας στην υπηρεσία eBanking. Για ακόμα μεγαλύτερη ασφάλεια κατά την διαδικασία εισόδου στην υπηρεσία eBanking, απαιτείται και η καταχώρηση της Ηλεκτρονικής Υπογραφής Συναλλαγής. Η Ηλεκτρονική Υπογραφή Συναλλαγής είναι μία μέθοδος ταυτοποίησης χρηστών που στηρίζεται στην δημιουργία κωδικών μιας χρήσης (one time passwords) οι οποίοι παράγονται από την ειδική συσκευή Security Token που παρέχει η Τράπεζα.

Η παραγωγή πραγματοποιείται με τη βοήθεια ισχυρών μαθηματικών αλγορίθμων και άλλων τυχαία μεταβαλλόμενων παραμέτρων, όπως για παράδειγμα η χρονική στιγμή χρήσης της συσκευής.

(β) Ταυτοποίηση κατά την πραγματοποίηση συναλλαγών

Η διαδικασία ταυτοποίησης του χρήστη από την Marfin Egnatia Bank δεν σταματάει εδώ. Για την πραγματοποίηση οποιασδήποτε οικονομικής συναλλαγής ή και

συναλλαγής που μεταβάλλει σημαντικά για σας στοιχεία (π.χ. αλλαγή PIN), απαιτείται η καταχώρηση της Ηλεκτρονικής Υπογραφής Συναλλαγής.

Προκειμένου όλες οι πληροφορίες που διακινούνται από τον υπολογιστή προς την Τράπεζα και αντιστρόφως να είναι απόρρητες, πρέπει να ταξιδεύουν σε κρυπτογραφημένη μορφή.

Η υπηρεσία eBanking υποστηρίζεται από το πρωτόκολλο επικοινωνίας SSL με κρυπτογράφηση 128bit. Η κρυπτογράφηση στα 128 bit θεωρείται πρακτικά αδύνατο να παραβιαστεί, δεδομένου ότι ένα σύγχρονο υπολογιστικό σύστημα θα χρειαζόταν αρκετά δισεκατομμύρια έτη για να διαβάσει τέτοια κρυπτογραφημένα δεδομένα. Μπορεί ο χρήστης να επιβεβαιώνει ότι βρίσκεται σε σελίδα με ενεργοποιημένη κρυπτογράφηση, εφόσον στην ηλεκτρονική διεύθυνση της σελίδας το «http» έχει μετατραπεί σε «https» (όπου s σημαίνει secure) και ταυτόχρονα υπάρχει το εικονίδιο με το λουκέτο στο κάτω μέρος της σελίδας αυτής.

Η πιστοποίηση παρέχεται στην Τράπεζα μέσω Πιστοποιητικού Αυθεντικότητας που εκδίδουν εξουσιοδοτημένες για το σκοπό αυτό ανεξάρτητες εταιρείες και διασφαλίζουν ότι κανείς άλλος δεν μπορεί να προσποιηθεί στον χρήστη ότι είναι η Τράπεζα και να υποκλέψει με τον τρόπο αυτό τις πληροφορίες του. Στην υπηρεσία eBanking έχει εγκατασταθεί το Πιστοποιητικό Αυθεντικότητας της VERISIGN. Η εμφάνιση του εικονιδίου με το λουκέτο στο κάτω δεξιά μέρος της οθόνης σας υποδηλώνει ότι είστε στην σωστή σελίδα. Προκειμένου να επιβεβαιωθεί η αυθεντικότητα της σελίδας του eBanking, μπορεί κάποιος να κάνετε κλικ στο σήμα της VERISIGN που υπάρχει στην οθόνη login της υπηρεσίας.

2.8 Ηλεκτρονικές επιταγές

Μια επιταγή χρησιμοποιείται για να μεταφέρει ένα μήνυμα προς την τράπεζα του αποστολέα για τη μεταφορά ενός χρηματικού ποσού συγκεκριμένης αξίας από το λογαριασμό του στον λογαριασμό κάποιου άλλου. Σε μια κοινωνία που συνεχώς εξελίσσεται η συνέχεια των παραδοσιακών επιταγών είναι οι ηλεκτρονικές επιταγές. Τέτοιου είδους επιταγές μπορούν και υπογράφονται και μεταβιβάζονται ηλεκτρονικά έχοντας όλες εκείνες τις ιδιότητες των κανονικών επιταγών. Οι ηλεκτρονικές επιταγές, όπως και οι κοινές μπορούν να διακριθούν σε πιστοποιημένες αλλά και σε ταξιδιωτικές επιταγές.

Όπως και με μια έντυπη επιταγή, η ηλεκτρονική αποστέλλεται στον παραλήπτη ο οποίος με τη σειρά του την επικυρώνει με την υπογραφή του και τη στέλνει στην τράπεζα προκειμένου να λάβει το αντίστοιχο ποσό. Η επιταγή αυτή στη συνέχεια επιστρέφεται στον αποστολέα ο οποίος τη χρησιμοποιεί σαν αποδεικτικό πληρωμής. Η ηλεκτρονική επιταγή είναι ένα ηλεκτρονικό έγγραφο το οποίο περιέχει τον αριθμό επιταγής, το όνομα του αποστολέα, τον αριθμό λογαριασμού του πληρωτή και το όνομα της τράπεζας. Επίσης, πρέπει να αναγράφονται το όνομα του δικαιούχου πληρωμής, δηλαδή του αποδέκτη, το πληρωτέο ποσό, η μονάδα του χρήματος που χρησιμοποιείται, η ημερομηνία λήξης, η ηλεκτρονική υπογραφή του πληρωτή και η ηλεκτρονική επικύρωση του δικαιούχου πληρωμής.

Οι ηλεκτρονικές επιταγές χρησιμοποιούν την τεχνολογία των ψηφιακών υπογραφών προκειμένου να πιστοποιηθούν. Τέτοιου είδους επιταγές θεωρούνται πιο ασφαλείς από τις έντυπες αφού ο αποστολέας μπορεί να προστατευτεί από μια πιθανή απάτη. Κάτι τέτοιο μπορεί να επιτευχθεί με την κρυπτογράφηση του αριθμού λογαριασμού του αποστολέα με το δημόσιο κλειδί της τράπεζας του με αποτέλεσμα να μην μπορεί να αποκαλυφθεί στον παραλήπτη ο αριθμός του λογαριασμού. Σε μια

διαδικασία πληρωμής μέσω ηλεκτρονικής επιταγής ο πελάτης παραγγέλνει κάποια προϊόντα από τον προμηθευτή και για την πληρωμή των ειδών αυτών αποστέλλει μια ηλεκτρονική επιταγή επικυρωμένη με την ψηφιακή του υπογραφή. Ο προμηθευτής γνωρίζοντας το δημόσιο κλειδί του αποστολέα είναι σε θέση να επιβεβαιώσει την ορθότητα της υπογραφής του και να επικυρώσει την επιταγή. Μετά την παραλαβή και την επικύρωση της ο έμπορος θα στείλει τα προϊόντα στον πελάτη. Στη συνέχεια η τράπεζα θα αποσύρει το ποσό πώλησης από τον λογαριασμό του πελάτη και μέσω του διατραπεζικού συστήματος το εν λόγω ποσό θα πιστωθεί στον λογαριασμό του προμηθευτή.

2.9Ηλεκτρονικό χρήμα

Οι περισσότεροι αναλυτές συμφωνούν στο ότι όσο το ηλεκτρονικό εμπόριο αυξάνεται, ταυτόχρονα αυξάνεται και η ανάπτυξη του ηλεκτρονικού χρήματος. Το ηλεκτρονικό χρήμα είναι το σύγχρονο μέσω πληρωμής μέσω του διαδικτύου. Η χρήση του για την αγορά προϊόντων τείνει να χρησιμοποιείται ολοένα και περισσότερο από τους καταναλωτές καθώς η διαδικασία ολοκληρώνεται πιο γρήγορα από τη συμπλήρωση όλων των στοιχείων μιας πιστωτικής κάρτας. Ως ηλεκτρονικό χρήμα, η Ευρωπαϊκή Κεντρική Τράπεζα ορίζει « την αποθήκευση χρηματικής αξίας σε ψηφιακή μορφή μέσω μιας συσκευής που μπορεί να χρησιμοποιηθεί ευρέως για την πραγματοποίηση πληρωμών σε δίκτυα χωρίς τη χρήση τραπεζικών λογαριασμών. Το ηλεκτρονικό χρήμα θα λειτουργεί ως προπληρωμένο υπόθεμα. Ενώ τα δίκτυα θα είναι είτε ανοιχτά δηλαδή θα μετατρέπουν την άμεση μεταφορά χρημάτων μεταξύ υποθεμάτων είτε κλειστά όπου η χρέωση του υποθέματος θα γίνεται στον τραπεζικό λογαριασμό αποκλειστικά.»

Με τον όρο ηλεκτρονικό χρήμα γενικά περιγράφεται η οποιαδήποτε μορφή μεταφοράς χρήματος μεταξύ δύο ή παραπάνω μερών η οποία γίνεται με ψηφιακό τρόπο χωρίς τη μεσολάβηση κάποιου υλικού μέσου.

Το ηλεκτρονικό χρήμα διακρίνεται σε δύο κατηγορίες, είτε με κάρτες αποθηκευμένης αξίας είτε με ειδικό λογισμικό. Όσον αφορά την πρώτη περίπτωση η κάρτα περιέχει ένα συγκεκριμένο ποσό το οποίο έχει προπληρώσει ο κάτοχος της. Μια κάρτα μπορεί να είναι είτε ανώνυμη είτε ονοματική. Ο κάτοχος της κάρτας μπορεί να της καταβάλλει το ποσό που επιθυμεί. Για λόγους ασφαλείας του ιδιοκτήτη της η κάρτα προστατεύεται από έναν κωδικό. Από την άλλη πλευρά, στα σχήματα μέσω λογισμικού πραγματοποιείται η έκδοση ηλεκτρονικών νομισμάτων από έναν παροχέα υπηρεσιών πληρωμών, συνήθως είναι η τράπεζα. Τα ηλεκτρονικά νομίσματα αυτά είναι αποθηκευμένα σε ένα ηλεκτρονικό πορτοφόλι στον υπολογιστή του χρήστη τα οποία μπορεί να τα διαθέσει για να πραγματοποιήσει τις διάφορες αγορές του. Βασικό πλεονέκτημα του ηλεκτρονικού χρήματος είναι το ότι ο αγοραστής διατηρεί την ανωνυμία του.

Το ηλεκτρονικό χρήμα θα πρέπει να έχει τα παρακάτω χαρακτηριστικά:

- Ανωνυμία του αγοραστή

- Ικανοποιητικό επίπεδο ασφαλείας
- Ευρεία αποδοχή
- Ευχρηστία
- Μεταφερσιμότητα από μία μορφή χρήματος σε μια άλλη πχ από ηλεκτρονικά σε μετρητά και αντίστροφα
- Διαιρετότητα
- Σταθερή αξία

Σε μια συναλλαγή όπου χρησιμοποιείται ηλεκτρονικό χρήμα, ο πελάτης έχει προμηθευτεί ψηφιακά νομίσματα από την τράπεζα ή από κάποιον άλλο οργανισμό έκδοσης ηλεκτρονικών νομισμάτων. Με τα νομίσματα ο πελάτης μπορεί να κάνει συναλλαγές μέσω διαδικτύου. Τα ψηφιακά νομίσματα χρησιμοποιούνται κυρίως για συναλλαγές χαμηλού κόστους (αγαθών ή υπηρεσιών) για αυτό και ο έμπορος δίνει τα προϊόντα χωρίς να ζητήσει πρώτα έγκριση πληρωμής. Στη συνέχεια ο έμπορος πρέπει να στείλει αίτημα εξαγοράς του ποσού στη τράπεζα όπου μέσω του διατραπεζικού δικτύου η τράπεζα του εξαργυρώνει τα νομίσματα στον οργανισμό πιστώνοντας στον λογαριασμό του εμπόρου το ποσό. Προκειμένου ο κάθε οργανισμός να εξασφαλίσει ότι το κάθε νόμισμα θα χρησιμοποιηθεί μία και μόνο φορά καταγράφει τον αύξοντα αριθμό του νομίσματος τη στιγμή που ξοδεύεται. Αν διαπιστωθεί από το σύστημα ότι χρησιμοποιούνται τα νομίσματα διπλή φορά τότε δηλώνει απάτη, ακυρώνει το νόμισμα πριν τη συναλλαγή και στη συνέχεια ειδοποιεί τον προμηθευτή.

2.10 Ηλεκτρονικό πορτοφόλι

Το ηλεκτρονικό πορτοφόλι είναι ένα νέο μέσο πληρωμών το οποίο μπορεί να προσφέρει πολλά πλεονεκτήματα στους καταναλωτές αλλά και στους εμπόρους. Το ηλεκτρονικό πορτοφόλι διευκολύνει τις συναλλαγές μέσω του ηλεκτρονικού εμπορίου και γι αυτό τείνει να αντικαταστήσει ένα μεγάλο μέρος των καθημερινών μικροσυναλλαγών χαράσσοντας έτσι πορεία προς την αντικατάσταση των μετρητών.

Το ηλεκτρονικό πορτοφόλι διακρίνεται σε δύο είδη, τις προπληρωμένες κάρτες και το ειδικό λογισμικό. Οι προπληρωμένες κάρτες έχουν το μέγεθος των πιστωτικών καρτών και χρησιμοποιούνται για τις συναλλαγές μέσω διαδικτύου. Μπορούν και αυτές να είναι είτε ονομαστικές είτε ανώνυμες για τη διευκόλυνση του αγοραστή αποκρύπτοντας έτσι τα στοιχεία του. Στην περίπτωση που η κάρτα είναι ονομαστική ο πελάτης θα πρέπει να πάρει από την τράπεζα μια κάρτα στην οποία θα έχει μεταφερθεί ένα ποσό του υπολοίπου του λογαριασμού του. Για λόγους ασφαλείας αυτές οι κάρτες τείνουν να είναι έξυπνες κάρτες. Στην περίπτωση όπου η κάρτα είναι ανώνυμη ο κάτοχος τη χρησιμοποιεί εύκολα και ανώνυμα αφού το ποσό έχει προπληρωθεί κατά την αγορά της χωρίς να παρεμβαίνει η τράπεζα. Επιπλέον πλεονέκτημα της ανώνυμης σε σχέση με την ονομαστική είναι πως δεν μπορεί να μεταβιβαστεί σε άλλο άτομο. Η προπληρωμένη κάρτα αποτελεί έναν εναλλακτικό τρόπο πληρωμής για τους καταναλωτές οι οποίοι είναι αρκετά δύσπιστοι στη χρήση της πιστωτικής τους για τις πληρωμές μέσω διαδικτύου.

Το ειδικό λογισμικό από την άλλη αφορά έναν ειδικά διαμορφωμένο τύπο λογισμικού όπου αποθηκεύει χρηματική αξία όπως αναφέρθηκε με τη μορφή των ψηφιακών νομισμάτων. Τα νομίσματα αυτά είναι αποθηκευμένα στον υπολογιστή του χρήστη και χρησιμοποιούνται για τις ηλεκτρονικές συναλλαγές. Γενικά, το ηλεκτρονικό πορτοφόλι διαθέτει ένα συγκεκριμένο χρηματικό ποσό που μπορεί να

χρησιμοποιηθεί για αγορές σε ηλεκτρονικά καταστήματα όπου η τράπεζα συνεργάζεται. Το ηλεκτρονικό πορτοφόλι παρέχει μέγιστη ασφάλεια καθώς το ποσό χρέωσης δεν μπορεί να υπερβεί το ποσό που υπάρχει ήδη στο πορτοφόλι.

2.11 Οικονομικές Συναλλαγές Επιχείρησης- Κράτους

Φυσικά από τις σύγχρονες οικονομικές συναλλαγές δεν θα μπορούσε να λείπει η σχέση Επιχείρησης με το Κράτος (Business-to-Government, B2G) . Παρακάτω αναφέρονται οι τρόποι όπου μια επιχείρηση μπορεί να κάνει πιο γρήγορα τις πληρωμές της μέσω διαδικτύου. Οι πληρωμές αυτές αφορούν πληρωμή φόρων όπως ο φόρος Εισοδήματος Νομικών προσώπων, ο Φόρος Προστιθέμενης Αξίας (ΦΠΑ), ο φόρος Μισθωτών Υπηρεσιών (ΦΜΥ), η πληρωμή προστίμων και ασφαλιστικών εισφορών. Μια τέτοια υπηρεσία σημαίνει και είσπραξη χρηματικών ποσών από το κράτος ως αποτέλεσμα εμπορικής συναλλαγής.

Ενδεικτικά παρακάτω αναφέρονται οι πληρωμές που μπορεί να κάνει μια επιχείρηση στο Δημόσιο. Στον τομέα Άμυνα, Ασφάλεια, Δικαιοσύνη πληρωμές μπορούν να γίνουν για χορήγηση Άδειας σύστασης και έγκρισης καταστατικών της εταιρείας. Όσον αφορά το Κρατικό Εισόδημα, η Εργοδοτική Εισφορά γίνεται εύκολα και γρήγορα μέσω του υπολογιστή. Επίσης μπορεί να γίνει και πληρωμή για Οικοδομική Άδεια ή Επανασύνδεση ηλεκτρικού ρεύματος. Επιπλέον μπορεί να καταβληθεί το Τέλος Έγκρισης Τύπου Μηχανημάτων έργων.

Κάθε εταιρεία οφείλει να καταβάλλει στη ΔΟΥ στην οποία ανήκει κάποιο ποσό. Οι πληρωμές της επιχείρησης είναι ανάλογες με αυτές που καταβάλλουν οι πολίτες, τόσο ως προς τα αντικείμενα των πληρωμών όσο και ως προς τους τρόπους πληρωμής. Όπως προαναφέρθηκε, τα αντικείμενα πληρωμών δε διαφέρουν μεταξύ φυσικών προσώπων και επιχειρήσεων όταν πρόκειται για πληρωμές στις Δημόσιες Οικονομικές Υπηρεσίες. Παρόλα αυτά διαφέρει, το πλήθος, η συχνότητα και η οικονομική αξία των συναλλαγών. Οι τρόποι πληρωμής της Δ.Ο.Υ επίσης δε διαφέρουν για τις επιχειρήσεις σε σχέση με τους πολίτες. Όλες οι οφειλές μπορούν να πληρωθούν στο ταμείο της ΔΟΥ με μετρητά, με επιταγές, ή μέσω των ειδικών μηχανημάτων POS που έχουν εγκατασταθεί στις ΔΟΥ.

Οι εισπράξεις χρηματικών ποσών της επιχείρησης από τις δημόσιες υπηρεσίες σε πολλές περιπτώσεις ταυτίζονται με αυτές των πολιτών, κατ' αναλογία των πληρωμών, τόσο ως προς τα αντικείμενα των πληρωμών όσο και ως τους τρόπους πληρωμής. Στην περίπτωση των επιχειρήσεων που δεν είναι ατομικές, η επιχείρηση πρέπει να εκπροσωπείται από τον νόμιμο εκπρόσωπο της. Έτσι ενώ στην πράξη κάτι τέτοιο χρειάζεται μια πληθώρα διοικητικών εγγράφων και φυσική παρουσία στη ΔΟΥ, στις ηλεκτρονικές υπηρεσίες απαιτεί εξειδικευμένες τεχνολογίες ταυτοποίησης και αυθεντικοποίηση των χρηστών μέσω της κρυπτογράφησης.

Πληρωμές προς τις Τελωνειακές Υπηρεσίες

Η κυκλοφορία και η κατανάλωση των εμπορευμάτων που εισάγονται στην Ευρωπαϊκή Ένωση από τρίτες χώρες, πραγματοποιείται με την υποβολή τελωνειακής διασάφησης εισαγωγής στο τελωνείο ελέγχου των εμπορευμάτων. Κάτι τέτοιο συνεπάγεται την εφαρμογή μέτρων εμπορικής πολιτικής και την επιβολή των νόμιμων οφειλόμενων δασμών. Αφού πραγματοποιηθεί η διασάφηση των εμπορευμάτων γίνεται υπολογισμός των δασμών και των φόρων που πρέπει να

πληρωθούν για να εκδοθεί η άδεια παράδοσης των εμπορευμάτων και να τεθούν τα εμπορεύματα πλέον σε ελεύθερη κυκλοφορία. Οι τελωνιακές υπηρεσίες που παρακολουθούν την αποθήκευση και των εκτελωνισμό των προϊόντων επιβαρύνονται με Ειδικό Φόρο Κατανάλωσης. Ειδικό Φόρο Κατανάλωσης έχουν προϊόντα όπως τα αυτοκίνητα, τα πετρελαιοειδή, τα καπνικά και τα αλκοολούχα. Επιπλέον, στις τελωνειακές υπηρεσίες βεβαιώνεται καθημερινά πληθώρα χρεών προς τους πολίτες ή τις επιχειρήσεις οι οποίες μπορεί να αφορούν συμπληρωματικές χρεώσεις δασμών, φόρων και λοιπών επιβαρύνσεων που διέφυγαν της καταβολής, πρόστιμα από τις τελωνειακών παραβάσεων, κλπ. Οι οφειλές αυτές καταβάλλονται σε μία ή σε περισσότερες δόσεις

Κρατικές Προμήθειες

Η διαδικασία των κρατικών προμηθειών επιβαρύνει χρονικά τον όλο κύκλο προμήθειας από την προκήρυξη έως την πληρωμή του προμηθευτή, με αποτέλεσμα η ηλεκτρονικοποίηση της πληρωμής να μην προσθέτει ουσιαστικά πλεονεκτήματα και βελτίωση της παραγωγικότητας στην συνολική διαδικασία .Όμως, λόγω του ότι ο ευρύτερος δημόσιος τομέας είναι ο μεγαλύτερος αγοραστής και με βάση ότι κάθε προμήθεια ενέχει και οικονομική συναλλαγή ανάμεσα στο κράτος και την επιχείρηση, η σημασία της αυτοματοποίησης των προμηθειών και ειδικότερα της οικονομικής συναλλαγής αποτελεί ένα μεγάλο ποσοστό αυτοματοποίησης τόσο του συνολικού αριθμού, όσο και του συνολικού όγκου των οικονομικών συναλλαγών κράτους και επιχειρήσεων με ιδιαίτερο χαρακτηριστικό την κατεύθυνση ροής του χρήματος από το κράτος προς την επιχείρηση.

Η οικονομική συναλλαγή στον χώρο των κρατικών προμηθειών ανάμεσα σε κράτος και επιχείρηση έχει μερικά συγκεκριμένα χαρακτηριστικά που αναδεικνύουν την πολυπλοκότητα του προβλήματος, αλλά προσφέρονται ταυτόχρονα και σαν ευκαιρία για συνδυαστική εφαρμογή ηλεκτρονικής διαδικασίας στο τελευταίο στάδιο της συναλλαγής. Επίσης, μεγάλο πλεονέκτημα για το δημόσιο είναι η ηλεκτρονικοποίηση των τιμολογίων και των παραστατικών ΔΑ , καθόσον οι διαδικασίες αυτές είναι συσχετιζόμενες, δηλαδή να τιμολογείται αυτό που παραδόθηκε ή ακόμη αυτό που παραγγέλθηκε.

Ηλεκτρονικές προμήθειες δημοσίου

Η ΕΕ έχει δραστηριοποιηθεί στον τομέα των ηλεκτρονικών προμηθειών περισσότερο από μία 10ετία. Τα βασικά χαρακτηριστικά και οι καινοτομίες από τις οδηγίες που αφορούν θέματα ηλεκτρονικών προμηθειών είναι τα ακόλουθα:

- Ενσωμάτωση Ηλεκτρονικών μεθόδων επικοινωνίας ανάμεσα στο δημόσιο και την αγορά, με βάσει τις οποίες μειώνονται οι χρόνοι από την αναγγελία έως την διεξαγωγή του διαγωνισμού.
- Παρουσίαση νέων τρόπων «σύναψης συμβάσεων» οι οποίοι είναι ηλεκτρονικοί και σκοπό έχουν την ευκολία των επιχειρήσεων.

Μοντέλα Ηλεκτρονικών Πληρωμών

Σήμερα, κατά τη διεξαγωγή μιας πληρωμής για τη διεκπεραίωση μιας υπηρεσίας στο δημόσιο τομέα με ηλεκτρονικό ή συμβατικό τρόπο, πραγματοποιούνται τα εξής εναλλακτικά σενάρια:

- Πληρωμή απ' ευθείας στο Δημόσιο Φορέα με τη μεσολάβηση επιλεγμένων τραπεζών: Ο πολίτης πραγματοποιεί στις εγκαταστάσεις του δημόσιου φορέα με συμβατικό τρόπο την πληρωμή απ' ευθείας στο δημόσιο φορέα ή αποκτά πρόσβαση στο Δημόσιο Διαδικτυακό Τόπο του Φορέα και πραγματοποιεί μια ηλεκτρονική πληρωμή. Υπάρχει διεπαφή για την ηλεκτρονική πληρωμή στη Διαδικτυακή Πύλη του Δημόσιου Φορέα και έχει αναπτυχθεί σε συνεργασία με επιλεγμένες τράπεζες.
- Πληρωμή έμμεσα με τη μεσολάβηση επιλεγμένων τραπεζών: Ο πολίτης πραγματοποιεί με συμβατικό τρόπο την πληρωμή πηγαίνοντας στην τράπεζα ή αποκτά πρόσβαση σε υπηρεσίες Ηλεκτρονικής Τραπεζικής επιλεγμένων τραπεζών και πραγματοποιεί μια ηλεκτρονική πληρωμή. Ο πολίτης πρέπει να γνωρίζει εκ των προτέρων τον κωδικό πληρωμής, τον οποίο γνωστοποιεί στην τράπεζα. Η ΔΙΑΣ αποστέλλει στον αρμόδιο δημόσιο φορέα τις συγκεντρωτικές καταστάσεις πληρωμών ανά συμφωνημένα χρονικά διαστήματα.

Σενάρια Διεξαγωγής Πληρωμών στο Δημόσιο Τομέα

Τα Μοντέλα Ηλεκτρονικών Πληρωμών που προκύπτουν για το δημόσιο τομέα διακρίνονται σε 4 κατηγορίες με βάση την αρχιτεκτονική που ακολουθούν κατά τη λειτουργία τους, δηλαδή: αν υποστηρίζουν το συντονισμό των ηλεκτρονικών πληρωμών σε κεντρικό επίπεδο, ανά θεματική ενότητα (Κεντρικά Συστήματα Πληρωμών) ή προωθούν κατανεμημένο συντονισμό (Κατανεμημένα Συστήματα Πληρωμών). Επίσης χωρίζονται σε: μεσολάβηση της ΔΙΑΣ ως Οργανισμού Εκκαθάρισης Οικονομικών Συναλλαγών που να αποτελεί τη μοναδική διεπαφή με το δημόσιο ή όχι. Τα μοντέλα ηλεκτρονικών πληρωμών μπορούν είτε να αξιοποιήσουν τη δυνατότητα χρέωσης / πίστωσης κάποιου λογαριασμού (account-based) ή να στηρίζονται στην ανταλλαγή ηλεκτρονικού χρήματος που υπάρχει σε κάποιο ηλεκτρονικό πορτοφόλι (token-based) και ενδέχεται να αφορούν πληρωμές σημαντικών ποσών ή μικροπληρωμές.

Κεντρικοποιημένη Διεξαγωγή Ηλεκτρονικών Πληρωμών στο Δημόσιο Τομέα μέσω ΔΙΑΣ

Το Μοντέλο Κεντρικοποιημένης Διεξαγωγής Ηλεκτρονικών Πληρωμών στο Δημόσιο Τομέα με τη μεσολάβηση της ΔΙΑΣ ως Οργανισμού Εκκαθάρισης Οικονομικών Συναλλαγών προβλέπει την πραγματοποίηση ηλεκτρονικών πληρωμών από και προς το Δημόσιο Τομέα με τη βοήθεια Κεντρικών Πληροφοριακών Συστημάτων Πληρωμών που δημιουργούνται ανά Θεματική Ενότητα (π.χ. για Ασφαλιστικά Ταμεία, για Δήμους, για τις Δ.Ο.Υ.). Ο πολίτης ή η επιχείρηση που θέλει να διεκπεραιώσει μια υπηρεσία ηλεκτρονικής διακυβέρνησης που περιλαμβάνει ηλεκτρονική συναλλαγή απευθύνεται στην Κεντρική Κυβερνητική Πύλη (Ερμής) ή στη Διαδικτυακή Πύλη του Δημόσιου Φορέα που παρέχει την υπηρεσία μέσω πολλαπλών καναλιών πρόσβασης (για παράδειγμα, μέσω διαδικτύου ή μέσω κινητού τηλεφώνου). Ενημερώνεται για τη διαδικασία διεκπεραίωσης της υπηρεσίας μέσω

κατάλληλης διεπαφής της Διαδικτυακής Πύλης με το Ληξιαρχείο Διαλειτουργικότητας και μπορεί να πραγματοποιήσει την ηλεκτρονική οικονομική συναλλαγή από την Κεντρική Κυβερνητική Πύλη (Ερμής) ή στη Διαδικτυακή Πύλη του Δημόσιου Φορέα, που αναλαμβάνουν με τη σειρά τους να διασυνδεθούν με το Κεντρικό Σύστημα Πληρωμών ανάλογα με τη θεματική ενότητα στην οποία εντάσσεται η υπηρεσία (π.χ. ασφάλιση, φορολογία). Το Κεντρικό Σύστημα Ηλεκτρονικών Πληρωμών στη συνέχεια αναλαμβάνει να επικοινωνήσει με τη ΔΙΑΣ προκειμένου να διαπιστώσει εάν τα στοιχεία πληρωμής είναι έγκυρα και αν μπορεί να πραγματοποιηθεί η συναλλαγή (π.χ. εάν υπάρχει διαθέσιμο υπόλοιπο σε κάποιο λογαριασμό ή ηλεκτρονικό πορτοφόλι). Στη συνέχεια ενημερώνει το σύστημα του Δημοσίου φορέα τον οποίο αφορά η πληρωμή μόλις πραγματοποιηθεί. Το μοντέλο αυτό απευθύνεται κατά κύριο λόγο σε σχετικά ώριμους τεχνολογικά φορείς που έχουν ήδη πραγματοποιήσει σημαντικές επενδύσεις τόσο σε υλικοτεχνικό εξοπλισμό όσο και σε κατάρτιση επιχειρησιακών στελεχών πληροφορικής ώστε να μπορέσει να εξωτερικεύσει με σωστό, δομημένο και ασφαλή τρόπο συγκεκριμένες όψεις των υπηρεσιών ηλεκτρονικής διακυβέρνησης και των πληρωμών που εμπλέκουν στα Κεντρικά Συστήματα Ηλεκτρονικών Πληρωμών με τρόπο συμβατό με το Πλαίσιο Ηλεκτρονικής Διακυβέρνησης.

Κεντρικοποιημένη Διεξαγωγή Ηλεκτρονικών Πληρωμών στο Δημόσιο Τομέα χωρίς τη μεσολάβηση της ΔΙΑΣ

Το μοντέλο αυτό προβλέπει την πραγματοποίηση ηλεκτρονικών πληρωμών από και προς το Δημόσιο Τομέα με τη βοήθεια Κεντρικών Πληροφοριακών Συστημάτων Ηλεκτρονικών Πληρωμών που δημιουργούνται ανά Θεματική Ενότητα. Και σε αυτή την περίπτωση ο πολίτης ή η επιχείρηση που θέλει να πραγματοποιήσει μια ηλεκτρονική συναλλαγή απευθύνεται στην Κεντρική Κυβερνητική Πύλη (Ερμής) ή στη Διαδικτυακή Πύλη του Δημόσιου Φορέα, από την οποία ενημερώνεται για τη διαδικασία διεκπεραίωσης της υπηρεσίας μέσω κατάλληλης διεπαφής της Διαδικτυακής Πύλης με το Ληξιαρχείο Διαλειτουργικότητας και μπορεί να πραγματοποιήσει την ηλεκτρονική οικονομική συναλλαγή από την Κεντρική Κυβερνητική Πύλη (Ερμής) ή στη Διαδικτυακή Πύλη του Δημόσιου Φορέα, που αναλαμβάνουν με τη σειρά τους να διασυνδεθούν με το Κεντρικό Σύστημα Ηλεκτρονικών Πληρωμών ανάλογα με τη θεματική ενότητα στην οποία εντάσσεται η υπηρεσία (π.χ. ασφάλιση, φορολογία). Και σε αυτή την περίπτωση το Κεντρικό Σύστημα Ηλεκτρονικών Πληρωμών αναλαμβάνει να διαπιστώσει αν τα στοιχεία της πληρωμής ισχύουν και στη συνέχεια να ενημερώσει το σύστημα του Δημόσιου Φορέα τον οποίο αφορά η πληρωμή ότι όντως πραγματοποιήθηκε. Το πλεονέκτημα αυτής της μεθόδου είναι πως οι πληρωμές μπορούν να πραγματοποιηθούν άμεσα μέσω των τραπεζών χωρίς τη μεσολάβηση της ΔΙΑΣ. Μειονέκτημα της μεθόδου είναι η πολυπλοκότητα του συστήματος.

Κατανεμημένη Διεξαγωγή Ηλεκτρονικών Πληρωμών στο Δημόσιο Τομέα μέσω ΔΙΑΣ

Το Μοντέλο Κατανεμημένης Διεξαγωγής Ηλεκτρονικών Πληρωμών στο Δημόσιο Τομέα με τη μεσολάβηση της ΔΙΑΣ ως Οργανισμού Εκκαθάρισης Οικονομικών Συναλλαγών υποστηρίζει την ταυτόχρονη λειτουργία και συνύπαρξη

πολλαπλών Συστημάτων Πληρωμών που συντηρούνται «τοπικά» από Φορείς οι οποίοι παρέχουν πολλές υπηρεσίες και διαθέτουν το απαιτούμενο υπόβαθρο σε τεχνογνωσία και τεχνολογικές υποδομές. Στην περίπτωση αυτή, οι επιμέρους Δημόσιοι Φορείς αξιοποιούν τη διεπαφή με το σύνολο των τραπεζών που παρέχει ένας Οργανισμός Εκκαθάρισης Οικονομικών Συναλλαγών, όπως το ΔΙΑΣ. Το μοντέλο αυτό είναι πιο κοντά στη φιλοσοφία των Δημοσίων Φορέων και επιλύει μια σειρά από τα προβλήματα που δημιουργούνται στα παραπάνω μοντέλα αφού οι Δημόσιοι Φορείς είναι υπεύθυνοι για τη διενέργεια των πληρωμών αλλά και για την ανάπτυξη των συστημάτων που υποστηρίζουν.

Κατανεμημένη Διεξαγωγή Ηλεκτρονικών Πληρωμών στο Δημόσιο Τομέα χωρίς τη μεσολάβηση της ΔΙΑΣ

Το τελευταίο μοντέλο διεξαγωγής ηλεκτρονικών πληρωμών αφορά την ταυτόχρονη λειτουργία και συνύπαρξη πολλαπλών Συστημάτων Ηλεκτρονικών Σύστημα Ηλεκτρονικής Διακυβέρνησης που συντηρούνται «τοπικά» από Φορείς οι οποίοι παράλληλα αναπτύσσουν κατάλληλες τεχνολογικές υποδομές για τη διασύνδεσή τους με κάθε τράπεζα ξεχωριστά. Τα συστήματα αυτά δίνουν την δυνατότητα ηλεκτρονικών πληρωμών με συγκεκριμένες τράπεζες.

2.12 Οικονομικές συναλλαγές Πολίτη-Κράτους

Ο πολίτης πλέον συναλλάσσεται με το κράτος δηλαδή στην άμεση κατανάλωση ηλεκτρονικών υπηρεσιών από τον πολίτη για προσωπική κυρίως χρήση. Τέτοιες υπηρεσίες είναι κυρίως πληρωμή φόρων, όπως ο φόρος εισοδήματος, προστίμων, κλήσεων, παραβόλων αλλά και πληρωμών συντάξεων ή και μισθοδοσιών από δημόσιες υπηρεσίες. Τα όρια των σχέσεων αυτών συχνά είναι δυσδιάκριτα όταν η ίδια οντότητα αναλαμβάνει το ρόλο τόσο του πολίτη όσο και της επιχείρησης απέναντι στο κράτος. Για παράδειγμα, στην περίπτωση φυσικού προσώπου επιτηδευματία, όπου το ίδιο πρόσωπο υποβάλλει και πληρώνει δηλώσεις Φόρου Εισοδήματος Φυσικού Προσώπου αλλά και δηλώσεις Φόρου Προστιθέμενης Αξίας. Στην προσπάθεια το κράτος να μειώσει την γραφειοκρατία μέσω των υπηρεσιών ηλεκτρονικής διακυβέρνησης, αναλαμβάνει τον ρόλο μιας επιχείρησης η οποία προσφέρει πληθώρα ηλεκτρονικών υπηρεσιών στους πολίτες. Με αυτόν τον τρόπο βελτιώνει και την ποιότητα των παρεχόμενων υπηρεσιών και όπως μια επιχείρηση επιδιώκει να προωθήσει τη χρήση και την αποδοχή των υπηρεσιών αυτών από ένα όλο και μεγαλύτερο ποσοστό πολιτών. Προσπαθεί έτσι να μετατρέψει κάποιους ευκαιριακούς επισκέπτες των κυβερνητικών ισοτόπων σε τακτικούς πελάτες και χρήστες των κυβερνητικών ηλεκτρονικών υπηρεσιών.

Παρόλο που στους e-πολίτες συγκαταλέγονται κατηγορίες χρηστών όπως οι web-surfers που φαίνονται απρόθυμοι να αφήνουν στοιχεία της ταυτότητάς τους ή και προσωπικά δεδομένα στο διαδίκτυο ή οι ευκαιριακοί χρήστες των υπηρεσιών που βλέπουν με σκεπτικισμό την εκχώρηση προσωπικών δεδομένων σε τρίτους, οι e-πελάτες είναι συνήθως έμπειροι χρήστες του διαδικτύου οι οποίοι δε διστάζουν να συμπληρώνουν ηλεκτρονικές φόρμες με προσωπικά τους στοιχεία στο διαδίκτυο ειδικά όταν η εμπιστοσύνη και η ασφάλεια ενός κυβερνητικού φορέα κερδίσει την προσοχή τους. Αυτή η θεώρηση αποκτά ιδιαίτερο βάρος στο χώρο των ηλεκτρονικών οικονομικών συναλλαγών, όπου τα δεδομένα που ανταλλάσσονται μπορεί να είναι

ευαίσθητα οικονομικά δεδομένα ή στοιχεία που ως αντικείμενο υποκλοπής μπορεί να προωθήσουν μια οικονομική απάτη. Φυσικά δεν μπορεί να μη γίνει αναφορά και στις ιδιαιτερότητες στη συναλλαγή πολιτών-κράτους:

- Το κράτος σε σχέση με τον ιδιωτικό τομέα των εταιρειών υπολείπεται στο να εξυπηρετεί συγκεκριμένες ομάδες χρηστών λαμβάνοντας όμως υπόψιν και τα ιδιαίτερα χαρακτηριστικά τους. Αυτό συμβαίνει κυρίως στις συναλλαγές Πολιτών-Κράτους. Οι G2C κυβερνητικές ηλεκτρονικές υπηρεσίες απευθύνονται στο σύνολο των πολιτών και πρέπει να εξυπηρετούν αν όχι το σύνολο, τουλάχιστον ένα μεγάλο ποσοστό του συνόλου των αναγκών των πολιτών. Αυτό σημαίνει ότι σε όλα τα στάδια ανάπτυξης μιας κυβερνητικής ηλεκτρονικής υπηρεσίας, από την εκτίμηση των αναγκών έως την παραγωγική λειτουργία και την αποδοχή τους από τους αποδέκτες, θα πρέπει να λαμβάνονται υπ' όψη όλα τα διαφορετικά χαρακτηριστικά του πληθυσμού έτσι ώστε να μην αποκλείεται κανείς από τη χρήση τους.
- Επίσης, διαφέρει κατά πολύ ο βαθμός εξοικείωσής τους με τις νέες τεχνολογίες τηλεπικοινωνιών, πληροφορικής και διαδικτύου, με αποτέλεσμα η αύξηση της ανασφάλειας στη χρήση των ηλεκτρονικών υπηρεσιών, αλλά και η απροθυμία στην υιοθέτησή τους απέναντι στους παραδοσιακούς τρόπους συναλλαγών και τον πολλαπλασιασμό των προβλημάτων που σχετίζονται με τη χρήση τους, από ένα σημαντικό ποσοστό χρηστών.

Παρ' όλα αυτά το κράτος έχει να αντιμετωπίσει πολλές προκλήσεις για να μπορέσει να χτίσει μια σχέση συνεργασίας και όχι ανταγωνισμού με τον πολίτη. Τέτοιες προκλήσεις όπως η προσωποποίηση των υπηρεσιών, η βοήθεια και η υποστήριξη των χρηστών, η πρόσβαση στη χρήση των υπηρεσιών, η ελευθερία τεχνολογικών επιλογών κλπ. είναι θέματα που εξετάζονται κάτω από αυτό το πλαίσιο συνεργασίας και βελτίωσης.

Πληρωμές προς τους Οργανισμούς Τοπικής Αυτοδιοίκησης

Κάποιοι οργανισμοί παρέχουν στους πολίτες τους την δυνατότητα ηλεκτρονικής πληρωμής μέσω των διαδικτυακών τόπων τους. Χαρακτηριστικά παραδείγματα αποτελούν ορισμένοι δήμοι οι οποίοι αξιοποίησαν τα έργα των Δημοτικών Διαδικτυακών Πυλών που προκηρύχθηκαν και ολοκληρώθηκαν από την Κοινωνία της Πληροφορίας ΑΕ. Στη συνέχεια παρουσιάζονται ορισμένες υπηρεσίες που προσφέρουν τη δυνατότητα ηλεκτρονικών πληρωμών από τις δημοτικές διαδικτυακές πύλες όπως για παράδειγμα στο νομό Γρεβενών Πληρωμή Προστίμων Κώδικα Οδικής Κυκλοφορίας (Κ.Ο.Κ.). Μέσα από αυτήν την υπηρεσία ο πολίτης έχει τη δυνατότητα να πραγματοποιήσει τις πληρωμές των κλήσεων προστίμων ΚΟΚ που έχει από την Δημοτική Αστυνομία προς το Δήμο μέσω Web Banking μιας προκαθορισμένης τράπεζας ή μέσω του συστήματος Dias Debit της ΔΙΑΣ. Άλλο χαρακτηριστικό παράδειγμα μιας ηλεκτρονικής πληρωμής είναι η πληρωμή Λογαριασμών Ύδρευσης. Μέσα από αυτήν την υπηρεσία ο πολίτης μπορεί να

πραγματοποιήσει τις πληρωμές των λογαριασμών ύδρευσης προς το δήμο μέσω Web Banking σε όποια τράπεζα επιθυμεί.

Ηλεκτρονικές Πληρωμές on-line

Μέχρι πρόσφατα οι πληρωμές που συνοδεύουν τα ηλεκτρονικά υποβαλλόμενα στοιχεία γίνονται μέσω τραπεζών και υπάρχει μια χρονική υστέρηση στην ενημέρωση των εσωτερικών συστημάτων της Γ.Γ.Π.Σ. και των Δ.Ο.Υ.. Αυτή η χρονική καθυστέρηση μπορεί να είναι από μία ημέρα μέχρι και ένα μήνα στην περίπτωση του Φ.Π.Α. . Αυτό δυσχεραίνει την ομαλή διεκπεραίωση των διαδικασιών τόσο από τον πολίτη (π.χ. επιστροφή χρημάτων ή υποβολή τροποποιητικών δηλώσεων) όσο και από το δημόσιο (π.χ. ελεγκτικές διαδικασίες). Με την εισαγωγή των on-line ηλεκτρονικών πληρωμών και την άμεση ενημέρωση των συστημάτων, αυτά τα εμπόδια τείνουν να εξαφανιστούν.

Έργο TAXISnet

Με στόχο την ποιοτική και ποσοτική αναβάθμιση των ηλεκτρονικών υπηρεσιών φορολογικού περιεχομένου, την ευκολότερη και συντομότερη εξυπηρέτηση του πολίτη κατά τη διαδικασία της διοικητικής εξυπηρέτησης, την απεμπλοκή του από χρονοβόρες διαδικασίες, την απλοποίηση γραφειοκρατικών μηχανισμών και την εισαγωγή ψηφιακών (ηλεκτρονικών) υπηρεσιών και μορφών εξυπηρέτησης, η Γενική Γραμματεία Πληροφορικών Συστημάτων προχώρησε στην εκπόνηση του έργου TAXISnet. Στα πλαίσια του έργου προβλέπεται:

- Η ανάπτυξη εφαρμογών για την ασφαλή και αξιόπιστη παροχή ηλεκτρονικών υπηρεσιών και συναλλαγών προς τους Φορολογούμενους, ισοδύναμων με αυτές που σήμερα παρέχονται στις Δημόσιες Οικονομικές Υπηρεσίες (ΔΟΥ)
- Η υλοποίηση συστημάτων κέντρου δεδομένων που θα επιτρέπει την ασφαλή, αξιόπιστη και ενήμερη διασύνδεση των δεδομένων των ηλεκτρονικών υπηρεσιών TAXISnet με το Ολοκληρωμένο Πληροφοριακό Σύστημα TAXIS
- Διαδικτυακός κόμβος για την εξυπηρέτηση των χρηστών των ηλεκτρονικών υπηρεσιών (TAXISnet), με ενημερωτικό υλικό και επικοινωνιακά εργαλεία για την πληροφοριακή υποστήριξη του Πολίτη.

Συστήματα Υποστήριξης Συναλλαγών από τον Τραπεζικό Τομέα

Η πρώτη ηλεκτρονική τράπεζα εμφανίστηκε τον Οκτώβριο του 1995 στην Αμερική. Ήταν η Security First Network Bank, η οποία εξυπηρετούσε τους πελάτες της από το διαδίκτυο χωρίς να έχει δίκτυο καταστημάτων. Η ανάγκη πολλών πελατών των τραπεζών να πραγματοποιούν τις συναλλαγές τους με απλό, αλλά ασφαλή τρόπο, 24 ώρες το 24ωρο, 365 μέρες το χρόνο και χωρίς γεωγραφικό περιορισμό έγινε η αιτία δημιουργίας της συγκεκριμένης τράπεζας. Από εκείνη τη στιγμή και μετά, οι παραδοσιακές τράπεζες, οι οποίες μέσα από τα καταστήματα προωθούσαν προϊόντα και υπηρεσίες και εξυπηρετούσαν τις συναλλαγές των πελατών τους, ξεκίνησαν να αναπτύσσουν σε πιλοτικό επίπεδο, ως προς τα καταστήματα, δίκτυα εξυπηρέτησης, στα πρότυπα των ηλεκτρονικών τραπεζών. Δεν ήταν λίγες οι περιπτώσεις όπου

αναγκάστηκαν να προβούν σε ριζική αναθεώρηση των πληροφοριακών συστημάτων και ορισμένων επιχειρησιακών λειτουργιών τους προκειμένου να ανταποκρίνονται στα αιτήματα των πελατών που τους διαβιβάζονταν ηλεκτρονικά.

Σήμερα, έχει υιοθετηθεί ένας τρόπος λειτουργίας όπου δίνει έμφαση στη συνέργια ανάμεσα στα δίκτυα του φυσικού και του ηλεκτρονικού κόσμου, καθώς αναγνωρίστηκε η συμπληρωματικότητά τους: Τα ηλεκτρονικά δίκτυα και η Ηλεκτρονική Τραπεζική (e-Banking ή Internet banking) μπορούν άριστα να εξυπηρετήσουν επαναλαμβανόμενες τραπεζικές/χρηματοοικονομικές εργασίες, να πληροφορήσουν, να ειδοποιήσουν τον πελάτη, να τον διευκολύνουν στην προσωπική του χρηματοοικονομική διαχείριση. Αν και το κατάστημα παραμένει αναντικατάστατο στην προσέγγιση του πελάτη για την ανάλυση των αναγκών του, την επεξήγηση πολύπλοκων προϊόντων, την εκπαίδευση της πελατείας σε νέα προϊόντα και δίκτυα, και τέλος στην εξυπηρέτηση όσων συναλλαγών απαιτούν ακόμα τη φυσική παρουσία του πελάτη στο κατάστημα στην ουσία το e-banking έχει διευκολύνει τη ζωή των πολιτών.

Το e-Banking υπόσχεται την επανάσταση στις τραπεζικές συναλλαγές, καθώς μεταφέρει την ίδια την τράπεζα στην οθόνη του υπολογιστή μέσω Διαδικτύου παρέχοντας αμέτρητες δυνατότητες όπως άμεση πρόσβαση στους τραπεζικούς λογαριασμούς χωρίς χρέωση, διεκπεραίωσης συναλλαγών, παρακολούθησης της πορείας χαρτοφυλακίων, εξόφλησης λογαριασμών ΔΕΚΟ και πιστωτικών καρτών, αγοραπωλησία επενδυτικών προγραμμάτων, καθώς και πλήθος άλλων υπηρεσιών. Η εξάπλωση του e-banking είναι ραγδαία σε όλο τον κόσμο γι αυτό και οι ειδικοί εκτιμούν ότι στο μέλλον οι σύγχρονες τράπεζες θα δραστηριοποιούνται αποκλειστικά μέσω των νέων τεχνολογιών με τη βοήθεια του διαδικτύου.

Στην Ελλάδα, σήμερα, το τραπεζικό δίκτυο έχει τη δυνατότητα να συνάπτει συνεργασίες με οργανισμούς και επιχειρήσεις του δημοσίου και ιδιωτικού τομέα έτσι ώστε οι υπόχρεοι των τελευταίων να καταβάλλουν τις οφειλές τους κάνοντας χρήση των υποστηριζόμενων από τις Τράπεζες μεθόδων. Συνοπτικά λοιπόν οι Τράπεζες παρέχουν στους πελάτες τους μέσω του e-banking:

- Μέσα πληρωμών τα κυριότερα των οποίων είναι οι κάρτες, οι τραπεζικοί λογαριασμοί, οι επιταγές, κλπ.
- Εναλλακτικά δίκτυα εξυπηρετήσεως αυτών των μέσων πληρωμής όπως οι Αυτόματες Ταμειολογιστικές Μηχανές (ΑΤΜ), Αυτόματα Κέντρα Πληρωμών (ΑΚΠ), Ηλεκτρονικήτραπεζική διαδικτύου (Web Banking), τηλεφωνική τραπεζική (Phone Banking) κ.ά. Σύμφωνα με στοιχεία του Παρατηρητηρίου για την Κοινωνία της Πληροφορίας, το e-banking χρησιμοποιείται από 3 στις 4 επιχειρήσεις κυρίως για κίνηση λογαριασμού, πληρωμές ΦΠΑ & ΙΚΑ, μεταφορές χρημάτων και αποστολές εμβασμάτων και δεν διαφαίνεται ιδιαίτερη μεταβολή στη χρήση υπηρεσιών e-banking στο μέλλον.

Από την άλλη πλευρά σε ατομικό επίπεδο, η συντριπτική πλειοψηφία των πολιτών δεν χρησιμοποιεί το Διαδίκτυο για τραπεζικές συναλλαγές. Η διείσδυση είναι εξαιρετικά χαμηλή και απαιτείται προσπάθεια και κόπος για την αποδοχή του. Παρόλα αυτά, στο μέλλον διαφαίνεται άνοδος στη χρήση υπηρεσιών e-banking, ειδικά για πληρωμές λογαριασμών και υπάρχει αισιοδοξία για την αποδοχή του e-Banking λαμβάνοντας υπόψη και ένα κλασικό αντίστοιχο παράδειγμα, στο οποίο μεσολάβησε χρόνος από τη δημιουργία μέχρι την αποδοχή του από τους πολίτες, το πλέον διαδεδομένο σήμερα δίκτυο ηλεκτρονικής τραπεζικής των ΑΤΜ. Για την αποδοχή του χρειάστηκε μεγάλος κόπος και προσπάθεια, αλλά πλέον έχει καθιερωθεί

στη συνείδηση του πολίτη ως η συσκευή για ανάληψη μετρητών, αν και πολλοί αγνοούν τις υπόλοιπες υπηρεσίες που αυτό προσφέρει.

Όσον αφορά τις πληρωμές μέσω κινητού ή στη γλώσσα των τραπεζών, «κινητές πληρωμές», τις περισσότερες φορές η χρήση του όρου παραπέμπει στο δίκτυο εξυπηρέτησης της πληρωμής που είναι το δίκτυο της κινητής τηλεφωνίας, ενώ το μέσο πληρωμής είναι είτε ο τραπεζικός λογαριασμός είτε μια τραπεζική κάρτα. Η χρήση του κινητού τηλεφώνου με στόχο την εκτέλεση τηλεφωνικής τραπεζικής (phone banking) ή ηλεκτρονικής διαδικτυακής τραπεζικής (web / internet banking) έχοντας πρόσβαση σε μια ιστοσελίδα μέσω πρωτοκόλλου WAP ή άλλου, εμπίπτει σε αρκετούς από τους ορισμούς, που έχουν δοθεί για τις «κινητές πληρωμές». Στις περιπτώσεις όμως αυτές, το κινητό τηλέφωνο είναι απλώς η συσκευή για την πραγματοποίηση της πληρωμής, ενώ το μέσο πληρωμής και η μέθοδος λειτουργίας της πληρωμής (operating model) δεν διαφέρει σε τίποτα από τα άλλα δίκτυα ή συσκευές εξυπηρέτησης πληρωμών.

Συνοψίζοντας λοιπόν, με τον όρο «κινητές πληρωμές» νοούνται οι εξής μέθοδοι λειτουργίας:

- Χρήση μηνυμάτων κειμένου (SMS/ text message) για την αγορά ενός άυλου, συνήθως, αγαθού, όπως ήχοι κουδουνίσματος (ring tones), αγορά applications, μουσικής, κ.ά. και η πληρωμή γίνεται με αντίστοιχη αύξηση του λογαριασμού τελών χρήσεως της συνδέσεως κινητής τηλεφωνίας
- Πληρωμή μετά από αγορές σε ένα διαδικτυακό ιστοχώρο (κανονικό ηλεκτρονικό
- εμπόριο) και η πληρωμή μπορεί να γίνει είτε με τραπεζική κάρτα ή χρέωση στον τραπεζικό λογαριασμό αλλά και με αντίστοιχη αύξηση του λογαριασμού τελών χρήσεως της συνδέσεως κινητής τηλεφωνίας. Όταν η πληρωμή από τον τελικό καταναλωτή γίνεται μέσω του λογαριασμού τελών χρήσεως της συνδέσεως κινητής τηλεφωνίας θα πρέπει πρώτα να έχει διερευνηθεί από νομικής πλευράς σν επιτρέπεται ένας λογαριασμός παρόχου τηλεπικοινωνιακών υπηρεσιών να περιέχει παροχή μη τηλεπικοινωνιακών υπηρεσιών. Τέλος, υπάρχουν πιλοτικές, κυρίως, υλοποιήσεις, με ειδικές εφαρμογές λογισμικού κινητών τηλεφώνων για διαχείριση ηλεκτρονικού χρήματος.

Διαχείριση Πληρωμών από τις Τράπεζες

Όταν ένας Οργανισμός ή μια Εταιρεία εισπράττει πληρωμές, χρειάζεται να λάβει πληροφορία σε δύο διαφορετικά επίπεδα:

- Τη λογιστική πληροφορία όπου είναι απαραίτητη για την οικονομική διαχείρισή της. Η λογιστική πληροφορία αφορά:
- Το ποσό που εισπράττεται σε κάθε χρονική περίοδο (συνήθως σε ημερήσια βάση) με το οποίο πιστώνεται ο τραπεζικός λογαριασμός του Οργανισμού / Εταιρίας
- Το ποσό αμοιβής της Τράπεζας για την παροχή των υπηρεσιών εισπράξεων, με το οποίο χρεώνεται ο τραπεζικός λογαριασμός του Οργανισμού ή της εταιρείας ανάλογα
- Την ενημερωτική πληροφορία, όπου είναι απαραίτητη για την υπηρεσία τιμολογήσεως ή εισπράξεων ή διαχειρίσεως των σχέσεων με την πελατεία ή παρακολουθήσεως οφειλών, η οποία παρακολουθεί την εξόφληση των οφειλών των πελατών.

Οι πληρωμές γίνονται έτσι ώστε να εξασφαλίζουν:

- Την ταυτοποίηση της οφειλής με μοναδικό τρόπο προκειμένου να μην υπάρχει αμφισβήτηση και την οφειλή που εξοφλήθηκε και τον οφειλέτη που πλήρωσε.
- Τη δυνατότητα αυτόματης ενημέρωσης των πληροφοριακών συστημάτων (reconciliation) του λήπτη Οργανισμού ή Εταιρείας με τα στοιχεία της πληρωμής,

Ούτως ώστε οι πληροφορίες που είναι απαραίτητες για την παρακολούθηση των εισπράξεων να διαβάζονται αυτόματα και να εγγράφονται στην «καρτέλα» παρακολουθήσεως των οφειλών του κάθε πελάτη.

Η Έννοια του Κωδικού Πληρωμής

Σε κάθε τέτοια συναλλαγή παρέχεται και ένας κωδικός πληρωμής. Ο Κωδικός Πληρωμής είναι ένας αριθμός, το τελευταίο ψηφίο του οποίου είναι ψηφίο ελέγχου. Το ψηφίο ελέγχου παράγεται από ένα αλγόριθμο στον οποίο συμμετέχουν όλα τα ψηφία του κωδικού. Τα υπόλοιπα ψηφία αφορούν στην οφειλή ή/ και τον οφειλέτη, όπως την/τον αναγνωρίζει ο εκδότης του λογαριασμού. Ο κωδικός πληρωμής μπορεί να είναι για παράδειγμα ο αριθμός τιμολογίου όπως κωδικοποιείται από το πληροφοριακό σύστημα τιμολόγησης του Οργανισμού ή της Εταιρίας αλλά και ο κωδικός πελάτη όπως κωδικοποιείται στο πελατοκεντρικό σύστημα του Οργανισμού / Εταιρείας. Το ψηφίο του κωδικού μπορεί να αποτελείται από ένα σταθερό αριθμητικό πεδίο που θα υποδηλώνει είτε τον αριθμό/κωδικό του πελάτη στο πελατοκεντρικό σύστημα είτε εάν άλλο, μη μεταβλητό κωδικό, που θα αντιστοιχεί μονοσήμαντα στον αριθμό/κωδικό πελάτη. Εάν η εισπρακτέα εταιρεία αντιμετωπίζει κάθε οφειλή ως ξεχωριστή συναλλαγή με τον πελάτη, τότε, συνήθως, πρέπει να γνωρίζει ποια συγκεκριμένη οφειλή πληρώθηκε και ποια όχι, οπότε καθίσταται απαραίτητη η έκδοση διαφορετικού κωδικού για τη δημιουργία του κωδικού πληρωμής.

Σενάριο χρήσεως του κωδικού πληρωμής

Εκδίδεται το έντυπο λογαριασμού αναγράφει σε εμφανές σημείο τον κωδικό πληρωμής εξηγώντας και τη χρήση του, ειδικά στην περίπτωση που υπάρχουν διαφορετικοί κωδικοί πληρωμής ανά είδος πληρωμής. Ο πελάτης ενημερώνεται μέσω του εντύπου λογαριασμού και κάνοντας χρήση τόσο του κατάλληλου δικτύου εξυπηρετήσεως όσο και του μέσου πληρωμής, χρησιμοποιεί την εντολή πληρωμής για αυθημερόν ή μεταγενέστερη ημερομηνία εκτελέσεως. Κατά την εισαγωγή του κωδικού και των λοιπών στοιχείων πληρωμής από τον οφειλέτη σε κάποιο τραπεζικό δίκτυο εξυπηρετήσεως όπου καταχωρείται η εντολή πληρωμής του οφειλέτη, επανυπολογίζεται το ψηφίο ελέγχου του κωδικού πληρωμής για να μειωθεί σημαντικά η πιθανότητα λανθασμένης καταχωρήσεως του κωδικού. Η Τράπεζα καταγράφει την πίστωση στον λογαριασμό του δικαιούχου μαζί με τον κωδικό πληρωμής που χρησιμοποιήθηκε. Επειδή οι κωδικοί έχουν ένα ψηφίο ελέγχου, η πιθανότητα να καταχωρήθηκαν λάθος τα ψηφία του κωδικού πληρωμής αλλά το ψηφίο ελέγχου να είναι κατά τύχη σωστό είναι μικρότερη του 10%. Με διπλό ψηφίο ελέγχου, η πιθανότητα αυτή μειώνεται κάτω του 1%.Τέλος, η εταιρεία που πρέπει να εισπράξει τα χρήματα ενημερώνεται μέσω ηλεκτρονικού αρχείου από την Τράπεζα που εξυπηρετεί την είσπραξη των οφειλών για την εισπράξεις της προηγούμενης εργάσιμης ημέρας, το οποίο περιλαμβάνει το καταβληθέν ποσό και τον κωδικό πληρωμής.

2.13 Άλλες χρήσεις της Κρυπτογραφίας

Υπηρεσία χρονοσήμανσης

Εκτός από την ψηφιακή υπογραφή ένα άλλο ασφαλές μέσο που μπορεί να παρέχει ο Πάροχος Υπηρεσιών Πιστοποίησης είναι η υπηρεσία της χρονοσήμανσης. Η χρονοσήμανση χρησιμοποιώντας μια ηλεκτρονική σφραγίδα στο έγγραφο όπου αποστέλλει ένας χρήστης δίνει την ασφάλεια του εγγράφου προκειμένου αυτό να μη τροποποιηθεί ή αμφισβητηθεί καθορίζοντας παράλληλα τον ακριβή χρόνο αποστολής του μηνύματος. Τις περισσότερες φορές συναντάται στην ηλεκτρονική υποβολή δηλώσεων ή αιτήσεων στις δημόσιες υπηρεσίες, για παράδειγμα υποβολή καταστάσεων ΦΠΑ. Στη συγκεκριμένη περίπτωση δεν γίνονται δεκτές οι αιτήσεις μετά από μια καθορισμένη προθεσμία. Έτσι, όταν προκύψει πρόβλημα εκπρόθεσμης υποβολής ο αιτών μπορεί να αποδείξει την ακριβή ημερομηνία και ώρα υποβολής της δήλωσης.

Υπηρεσία αποθήκευσης μηνυμάτων

Η κατάθεση ενός εγγράφου ή μιας φορολογικής δήλωσης γίνονται πιο εύκολα και γρήγορα με τη χρήση ενός ηλεκτρονικού συμβολαιογράφου. Με την χρήση του μπορεί να πιστοποιηθεί ποιο κείμενο εστάλη αρχικά σε περίπτωση που χρειαστεί κάποιος φορολογικός έλεγχος. Το κείμενο το οποίο θα σταλεί πρέπει να πληροί τις παρακάτω προϋποθέσεις. Αρχικά, θα πρέπει να είναι ψηφιακά υπογεγραμμένο καθώς και κρυπτογραφημένο για να μην αλλοιωθεί το περιεχόμενο του. Όταν χρειαστεί επικείμενος έλεγχος τότε είναι απαραίτητο να προσκομιστεί και το ιδιωτικό κλειδί για την αποκρυπτογράφηση του. Τέλος, για την ασφαλέστερη αποστολή του το μήνυμα θα μπορούσε να είναι και χρονοσημασμένο.

Κρυπτογράφηση του τηλεφώνου

Επίσης μπορούν να κρυπτογραφηθούν όλα τα δεδομένα του τηλεφώνου του χρήστη όπως: τους Λογαριασμούς Google, τα δεδομένα εφαρμογών, τη μουσική και άλλα μέσα, τις πληροφορίες λήψης κ.ο.κ. Αν κρυπτογραφηθούν, θα πρέπει να εισαχθεί ένα αριθμητικό PIN ή έναν κωδικό πρόσβασης κάθε φορά που ενεργοποιείται το τηλέφωνό σας. Γνωρίζεται ότι αυτό είναι το ίδιο PIN ή κωδικός πρόσβασης που χρησιμοποιείται για να ξεκλειδωθεί το τηλέφωνό χωρίς κρυπτογράφηση και δεν μπορείτε να το οριστεί ανεξάρτητα.

Προειδοποίηση: Η κρυπτογράφηση δεν είναι αναστρέψιμη και μπορεί να την αναιρεθεί μέσω της εκτέλεσης επαναφοράς εργοστασιακών ρυθμίσεων από το κινητό η οποία ρύθμιση διαγράφει όλα τα δεδομένα.

Η κρυπτογράφηση παρέχει πρόσθετη προστασία στην περίπτωση κλοπής του τηλεφώνου και μπορεί να απαιτείται ή να ζητείται από ορισμένους οργανισμούς. Πριν να την ενεργοποίηση της, πρέπει ο χρήστης να απευθυνθεί στο διαχειριστή του

συστήματός. Σε πολλές περιπτώσεις, το PIN ή ο κωδικός πρόσβασης που ορίζεται για την κρυπτογράφηση ελέγχεται από το διαχειριστή συστήματος.

Ηλεκτρονική ψηφοφορία

Η ηλεκτρονική ψηφοφορία ή αλλιώς e-voting είναι το σύνολο των τεχνικών ηλεκτρονικών μέσων που χρησιμοποιούνται για την διεξαγωγή μιας ψηφοφορίας αλλά και για την καταμέτρηση των ψήφων αυτής. Ήδη σε χώρες όπως Ελβετία, Βραζιλία, Καναδά κ.α. το e-voting έχει αρχίσει να χρησιμοποιείται όχι μόνο σε πειραματικό επίπεδο. Στις ίδιες χώρες υπάρχει ανάλογο σύστημα και για τα δημοψηφίσματα αλλά και για την απογραφή(e-census). Οι τεχνικές που σχετίζονται με την ασφάλεια της ψηφοφορίας , όπως δηλαδή η μη διαστρέβλωση των αποτελεσμάτων αυτής αλλά και η ιδιωτικότητα της, προέρχονται από την επιστήμη της κρυπτογραφίας. Ως πρωτόκολλο ηλεκτρονικής ψηφοφορίας ορίζεται ένας κρυπτογραφικός αλγόριθμος ο οποίος καθορίζει τον τρόπο διενέργειας μιας εκλογικής διαδικασίας. Το πρωτόκολλο αυτό κρυπτογραφεί και υπογράφει ψηφιακά τις ψήφους και συγκεντρώνοντας τις ανώνυμα, αποτρέπει τη διαβλητότητα της διαδικασίας. Αν και η ηλεκτρονική ψηφοφορία χρησιμοποιεί έναν από τους πιο ασφαλείς αλγόριθμους δεν έχει βρεθεί λύση που να ικανοποιεί τις απαιτήσεις του συστήματος τόσο σε ασφάλεια όσο και σε αποδοτικότητα.

Υπάρχουν τρεις κατηγορίες διεξαγωγής της ψηφοφορίας και διακρίνονται σε: ψηφοφορίες που αφορούν ανώνυμο κανάλι, συνδυασμό ανώνυμου καναλιού και ψηφιακών υπογραφών αλλά και ομομορφικής κρυπτογράφησης.

Οι πρώτες δύο ψηφοφορίες είναι οι πιο γνωστές αφού δεν χρησιμοποιούν μεγάλες απαιτήσεις ασφαλείας υποστηρίζοντας έτσι όλους τους δυνατούς τρόπους διεξαγωγής της. Παρόλα αυτά, υπάρχουν και μειονεκτήματα για αυτές τις μεθόδους. Η τάση να επιβάλλουν στον χρήστη να δρα σε πολλούς γύρους, για παράδειγμα αρχικοποίηση, ψήφο, αρίθμηση, επαλήθευση, τυχόν διαμαρτυρία, αλλά και το ότι δεν περιλαμβάνουν το χαρακτηριστικό της καθολικής επιβεβαίωσης συγκαταλέγονται στα κατά τους. Από την άλλη πλευρά η ομομορφική κρυπτογράφηση μπορεί να ικανοποιήσει σε μεγάλο βαθμό τις απαιτήσεις ασφαλείας του συστήματος αφού η κάθε πληροφορία που εισέρχεται στο σύστημα είναι κρυπτογραφημένη. Φυσικά όμως κάτι τέτοιο προκαλεί μεγάλο κόστος επικοινωνίας στο δίκτυο αφού υποστηρίζουν συγκεκριμένο τύπο ψηφοδελτίων.

Το πρωτόκολλο της ηλεκτρονικής ψηφοφορίας θα πρέπει να πληροί τις παρακάτω ιδιότητες:

- Εμπιστευτικότητα: τα δεδομένα όπου αποθηκεύονται στις βάσεις δεδομένων για την ψηφοφορία να μην μπορούν να δοθούν σε τρίτους.
- Ακεραιότητα: τα δεδομένα που αποθηκεύονται στις βάσεις δεδομένων να μην μπορούν να διαστρεβλωθούν από τρίτους.
- Διαθεσιμότητα: τα δεδομένα είναι πάντα διαθέσιμα στους εξουσιοδοτημένους χρήστες του δικτύου.
- Αναγνωρισιμότητα: προκειμένου να εξακριβωθεί η ταυτότητα για τους εξουσιοδοτημένους χρήστες.
- Εξουσιοδότηση: τα εξουσιοδοτημένα μέλη μπορούν να δούν συγκεκριμένες πληροφορίες όχι το σύνολο αυτών.

- Μη δυνατότητα αποκύρηξης πράξης: κάθε χρήστης είναι υπεύθυνος για τις διενέργειες που θα πράξει στο σύστημα.
- Ιδιωτικότητα: δεν υπάρχει κανείς τρόπος με τον οποίο κάποιος μπορεί να συνάγει τις επιλογές ενός αξιολογητή.
- Επιλεξιμότητα: κάθε αξιολογητής μπορεί να αξιολογήσει μόνο μία φορά.
- Καθολική επιβεβαίωση: κάθε αξιολογητής μπορεί να επιβεβαιώσει ότι καταμετρήθηκε η ψήφος του.
- Δικαιοσύνη: πριν τη καταμέτρηση δεν γίνεται γνωστό οποιοδήποτε αποτέλεσμα της ψηφοφορίας.
- Ευστάθεια: να μπορεί να αυτοπροστατεύεται απο οποιοδήποτε λάθος ή σκόπιμη ενέργεια των συμμετεχόντων.
- Receipt- freeness: κάθε συμμετέχων δεν πρέπει να προσπαθήσει να πείσει κάποιον και να τον επηρεάσει.
- Ανεξαρτησία σύγκρουσης: δεν είναι δυνατόν δύο ή περισσότεροι χρήστες να πάρουν τα ίδια διακριτικά διαπίστευσης, με αυτόν τον τρόπο αποφεύγεται και το ενδεχόμενο διπλής ψηφοφορίας.

Κεφάλαιο Τρίτο - Μέτρα Ασφαλείας της Κρυπτογραφίας στις Οικονομικές Συναλλαγές

Για αυτό το κεφάλαιο χρησιμοποιήθηκε η εξής βιβλιογραφία:[1],[2],[4],[7],[8],[9],[11],[13],[14],[15],[16],[17],[18],[19],[20],[21]

3.1 Πρότυπα Ασφαλείας στις Οικονομικές Συναλλαγές

Εφαρμογή FIREWALL

Οι τοίχοι προστασίας (firewalls) αποτελούν μία πολύ αποτελεσματική μέθοδο προστασίας δικτύου. Στην ουσία πρόκειται για ένα σύστημα σχεδιασμένο να κάνει το δίκτυο προσβάσιμο με προσεκτικά ελεγχόμενους και παρακολουθούμενους τρόπους. Ένα σύστημα firewall επιτυγχάνει δύο στόχους: Παρέχει στους ανθρώπους της εταιρείας πρόσβαση στον παγκόσμιο ιστό, χωρίς ταυτόχρονα να επιτρέπει σε όλο τον κόσμο να παρακολουθεί παρανόμως και δεύτερον μπορεί να υψωθεί μεταξύ ενός ανέμπιστου τμήματος λογισμικού, του δημόσιου εξυπηρετητή ιστού και των ευαίσθητων πληροφοριών που ανήκουν στο ιδιωτικό δίκτυο της.

Βασική ιδέα ενός firewall

Η βασική ιδέα ενός firewall είναι γενικά απλή. Σε ένα παραδοσιακό ανοιχτό σύστημα, όλοι οι κεντρικοί υπολογιστές στο δίκτυο τοπικής περιοχής (Local Area Network - LAN) έχουν άμεση πρόσβαση στο Διαδίκτυο και είναι ισοδύναμα ευάλωτοι σε επιθέσεις από έξω.

Η ασφάλεια του τοπικού δικτύου εξαρτάται από την ασφάλεια του πιο αδύναμου κεντρικού υπολογιστή. Ένας απλός ανασφαλής κεντρικός υπολογιστής θα επιτρέψει σε ένα εισβολέα να εισέλθει. Όταν εισέλθει είναι εύκολο κλέβοντας τους λογαριασμούς νομίμων χρηστών, αντικαθιστώντας το λογισμικό του συστήματος με αντίγραφα και με άλλα τέτοια τεχνάσματα, να ανατρέψει άλλους κεντρικούς υπολογιστές στο χώρο. Όχι μόνο είναι δύσκολο να προστατευθεί ένα ανοιχτό σύστημα από επίθεση αλλά είναι δύσκολο να ανιχνευθεί η προσβολή του.

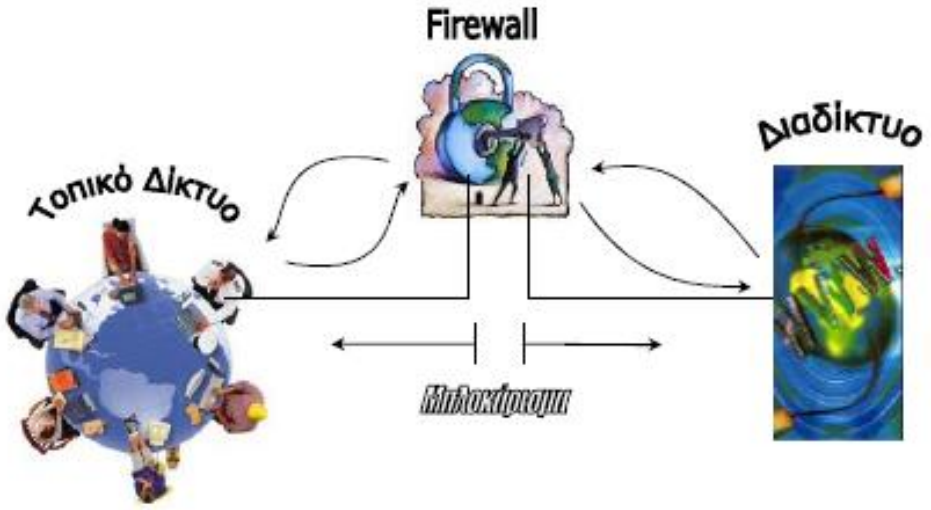
Τα firewalls αντιμετωπίζουν αυτό το πρόβλημα παρεμβάλλοντας μία ειδικά διαμορφωμένη μηχανή πύλης (gateway) ανάμεσα στον έξω κόσμο και στο εσωτερικό δίκτυο του χώρου. Η άμεση επαφή μεταξύ των κεντρικών υπολογιστών του εσωτερικού δικτύου και του εξωτερικού κόσμου απαγορεύεται. Αντίθετα όλη η κίνηση πρέπει πρώτα να πάει στην πύλη όπου το λογισμικό αποφασίζει αν η κίνηση μπορεί να επιτραπεί ή να απορριφθεί. Αυτό διαιρεί αποτελεσματικά το δίκτυο σε ένα "εσωτερικό" έμπιστο δίκτυο (δηλαδή το τοπικό) και σε ένα "εξωτερικό" ανέμπιστο δίκτυο (δηλαδή το διαδίκτυο).

Η ζώνη συνόρων μεταξύ των εσωτερικών και εξωτερικών δικτύων είναι γνωστή σαν "περίμετρος ασφάλειας". Τώρα η εργασία προστασίας του τοπικού δικτύου γίνεται πιο απλή καθώς αντί να προστατεύεται ένα ετερογενές σύνολο μεμονωμένων κεντρικών υπολογιστών από προσβολή, οι προσπάθειες επικεντρώνονται στην προστασία της απλής μηχανής πύλης του δικτύου. Αν η πύλη δικτύου είναι ασφαλής, το τοπικό δίκτυο είναι ασφαλές.

Υπάρχουν δύο βασικές υλοποιήσεις για συστήματα firewalls. Στην προσέγγιση "πύλη διπλής στέγης", η μηχανή του firewall που ονομάζεται "οχυρή θέση", έχει δύο κάρτες δικτύου, μία που συνδέεται με το εσωτερικό δίκτυο και μία που συνδέεται με το ανέμπιστο δίκτυο. Η μηχανή έχει ρυθμιστεί έτσι ώστε τα πακέτα δικτύου που φθάνουν στη μία κάρτα να μη βασίζονται στην άλλη. Εξ ορισμού τα δύο δίκτυα είναι εντελώς απομονωμένα. Παρόλα αυτά, επειδή υπάρχει πάντα η ανάγκη κάποιας επικοινωνίας μεταξύ των εσωτερικών και των εξωτερικών δικτύων, ειδικά προγράμματα, που ονομάζονται "μεσολαβητές" (proxies), τρέχουν στη μηχανή firewall. Η δουλειά ενός μεσολαβητή είναι να προωθήσει επιλεκτικά πληροφορίες από το ένα δίκτυο στο άλλο.

Οι μεσολαβητές μπορούν να καθορίσουν ποιά πακέτα δικτύου να προωθήσουν κοιτάζοντας τις διευθύνσεις προέλευσης και προορισμού, εξετάζοντας τον τύπο πακέτου, εξετάζοντας τις θύρες προέλευσης και προορισμού ή ακόμη ελέγχοντας τα περιεχόμενα που υπάρχουν μέσα στο πακέτο. Τα πακέτα δικτύου ποτέ δεν μεταφέρονται άμεσα. Τα δεδομένα τους εξάγονται και τοποθετούνται σε νέα πακέτα πριν μεταφέρουν τις πληροφορίες τους μέσω της πύλης δικτύου.

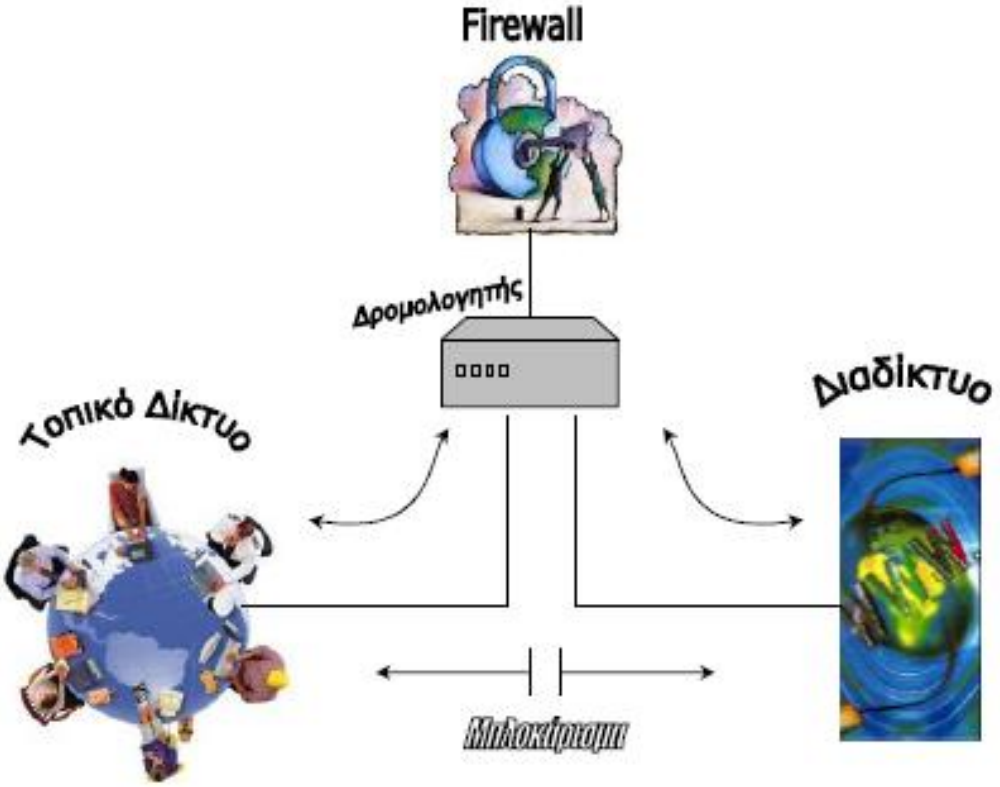
Σχεδιάγραμμα - Firewall σύμφωνα με την προσέγγιση "Πύλη διπλής στέγης"



Στην προσέγγιση "διαχωριστικού κεντρικού υπολογιστή πύλης" ένας δρομολογητής δικτύου χρησιμοποιείται για να ελέγξει την πρόσβαση στο εσωτερικό δίκτυο. Ο δρομολογητής περιορίζει την επικοινωνία μεταξύ των εξωτερικών και εσωτερικών δικτύων διασφαλίζοντας ότι τα δικτυακά πακέτα που ξεκινούν μέσα από το εξωτερικό δίκτυο μπορούν να φτάσουν μόνο όταν η καλά ασφαλισμένη μηχανή της οχυρής θέσης τα εξετάσει και με την παρουσία των μεσολαβητών, που τα αναμεταδίδουν στο εσωτερικό δίκτυο. Στις περισσότερες περιπτώσεις, οι μηχανές στο εσωτερικό δίκτυο είναι εντελώς αόρατες στο εξωτερικό.

Τα εξωτερικά πακέτα από το εσωτερικό δίκτυο είτε περιορίζονται στη μηχανή τοίχου προστασίας, όπου πάλι πρέπει να συνοδευτούν στο διαδίκτυο μέσω ενός προγράμματος μεσολάβησης ή επιτρέπεται να περάσουν άμεσα μέσω του δρομολογητή, αφού ικανοποιήσουν ορισμένους κανόνες φιλτραρίσματος για να προσδιορίσουν ότι είναι ασφαλή.

Σχεδιάγραμμα - Firewall σύμφωνα με την προσέγγιση " διαχωριστικού κεντρικού υπολογιστή πύλης"



Σε ένα καλά σχεδιασμένο σύστημα firewall, δεν υπάρχει καμία ουσιαστική διαφορά ανάμεσα στα συστήματα διπλής στέγης και διαχωριστικού κεντρικού υπολογιστή. Σε κάθε περίπτωση το εσωτερικό δίκτυο εμφανίζεται στον έξω κόσμο να περιέχει μία απλή καλά προστατευμένη μηχανή, τον κεντρικό υπολογιστή οχυρής θέσης. Όλη η εξερχόμενη κίνηση από το εσωτερικό δίκτυο στον έξω κόσμο εμφανίζεται να ξεκινά από την οχυρή θέση και όλη η εισερχόμενη κίνηση απευθύνεται σε αυτή τη θέση. Το λογισμικό στο οχυρό θέσης ελέγχει κάθε κομμάτι δεδομένων δικτύου που φτάνει, το καταγράφει και του επιτρέπει να περάσει αν ικανοποιεί το σύνολο κανόνων και ρυθμίσεων που έχουν οριστεί από τους διαχειριστές του firewall.

Πολλοί οργανισμοί έχουν εγκαταστήσει συστήματα firewalls που δεν είναι καθόλου firewalls. Είναι δρομολογητές δικτύου που έχουν διαμορφωθεί να σταματούν την επικίνδυνη κυκλοφορία δικτύου ενώ επιτρέπουν να προχωρήσει η ασφαλής κυκλοφορία του δικτύου. Αυτού του είδους το σύστημα μπορεί να είναι δύσκολο να διαχειριστεί αποτελεσματικά λόγω της δυσκολίας του να δημιουργήσει αποτελεσματικούς κανόνες φιλτραρίσματος. Ακόμη και μία φαινομενικά αβλαβής αλλαγή σε ένα πίνακα δρομολόγησης μπορεί να έχει αθέλητες επιδράσεις. Επειδή οι δρομολογητές δεν έχουν σχεδιαστεί βασικά για σκοπούς ασφάλειας, συνήθως δεν καταγράφουν τη δραστηριότητα του δικτύου, κάνοντας δύσκολο το να προσδιοριστεί αν το σύστημα δουλεύει κανονικά ή ακόμη και αν έχει προσβληθεί. Η ουσία μιας πολιτικής ασφάλειας ενός firewall έχει ενσωματωθεί στα φίλτρα που επιτρέπουν ή απαγορεύουν τη δίοδο στην κυκλοφορία δικτύου. Τα προγράμματα μεσολάβησης έρχονται σε δύο εκδόσεις. Υπάρχουν μεσολαβητές "επιπέδου εφαρμογής", που έχουν γραφτεί για συγκεκριμένα πρωτόκολλα επικοινωνίας.

Για παράδειγμα ένας μεσολαβητής επιπέδου εφαρμογής θα είναι υπεύθυνος για την προώθηση HTTP αιτήσεων μπρος και πίσω πάντα μέσω του firewall, ένας άλλος υπεύθυνος για FTP αιτήσεις και ένας τρίτος υπεύθυνος για το ηλεκτρονικό ταχυδρομείο. Επειδή οι μεσολαβητές επιπέδου εφαρμογής καταλαβαίνουν το νόημα

των πληροφοριών τις μεταδίδουν μπρος πίσω και μπορούν να εφαρμόσουν κανόνες φιλτραρίσματος με βάση τα περιεχόμενα των δικτυακών πακέτων.

Από την άλλη πλευρά, αν μια εταιρεία αποφασίσει να προστατεύσει τους υπαλλήλους της από πιθανούς κινδύνους ActiveX ελέγχων, θα μπορούσε να στήσει ένα HTTP μεσολαβητή για να εξετάσει κάθε HTML σελίδας που περνά την οχυρή θέση και να διαγράψει αθόρυβα τις αναφορές σε ActiveX. Οι μεσολαβητές επιπέδου εφαρμογής μπορούν επίσης να φιλτράρουν την κυκλοφορία δικτύου από τις IP διευθύνσεις των πλευρών αποστολής και παραλαβής, τις θύρες δικτύου σε οποιαδήποτε πλευρά της σύνδεσης και άλλα χαρακτηριστικά των επικεφαλίδων των πακέτων δικτύου.

Σε αντίθεση με τους μεσολαβητές επιπέδου εφαρμογής είναι οι μεσολαβητές "επιπέδου κυκλώματος", δηλαδή προγράμματα γενικού σκοπού που φέρονται στα πακέτα δικτύου σαν σε πολλά μαύρα κουτιά που θα προωθηθούν μέσω της οχυρής θέσης ή όχι. Αυτού του είδους ο μεσολαβητής μπορεί να φιλτράρει μόνο τη βάση της πληροφορίας επικεφαλίδας στα πακέτα δικτύου. Οι μεσολαβητές επιπέδου κυκλώματος μπορούν να απαγορέψουν πακέτα δικτύου που προέρχονται από απαγορευμένες πηγές, αλλά δεν μπορούν να κρυφοκοιτάξουν μέσα στο πακέτο να δουν αν ένα πακέτο, που φαίνεται νόμιμο, κρύβει μια επικίνδυνη δραστηριότητα. Το κύριο πλεονέκτημα των μεσολαβητών επιπέδου κυκλώματος είναι η γενικότητα και η ταχύτητά τους. Ένας μεσολαβητής μπορεί να διαχειριστεί πολλά πρωτόκολλα και είναι πιο γρήγοροι διότι η εργασία τους είναι λιγότερο έντονη υπολογιστικά.

Σε όλους τους τύπους των συστημάτων firewalls, η ασφάλεια του εσωτερικού δικτύου εξαρτάται από την ασφάλεια του κεντρικού υπολογιστή οχυρής θέσης. Κάποιος που αποκτά πρόσβαση στον τοίχο προστασίας ή είναι ικανός να αναδιαμορφώσει τα μέτρα ασφαλείας, το πιο πιθανό είναι να μπορεί να εισέλθει και σε άλλες μηχανές στο τοπικό δίκτυο. Σε συστήματα διαχωριστικού κεντρικού υπολογιστή, ο δρομολογητής είναι επίσης ένας πιθανός αδύνατος σύνδεσμος. Για να εμποδιστεί η έκθεση είτε της οχυρής θέσης είτε του κεντρικού υπολογιστή, τα firewalls είναι ειδικά διαμορφωμένα και διαχωρισμένα. Τυπικά, εκτελούν μία "σκληραγωγημένη" έκδοση των UNIX και NT λειτουργικών συστημάτων, από τις οποίες έχουν αφαιρεθεί διάφορα τρωτά σημεία. Τα firewalls δεν εκτελούν αχρείαστες υπηρεσίες, δεν περιέχουν ανέμπιστο λογισμικό και κρατούν μια ασφαλή καταγραφή όλης της δραστηριότητας.

Επιλέγοντας Ένα Σύστημα Firewall για Προστασία Οικονομικών Συναλλαγών

Αυτό που ακολουθεί είναι μία λίστα με τα σημαντικότερα χαρακτηριστικά που πρέπει να σκεφτεί ένας υποψήφιος αγοραστής ενός συστήματος firewall με σκοπό την προστασία ατόμων κατά τις οικονομικές τους συναλλαγές:

- Λειτουργικό Σύστημα. Τα προϊόντα firewalls που είναι διαθέσιμα εκτελούνται και στα δύο συστήματα UNIX και Windows NT. Κανένα από τα δύο λειτουργικά συστήματα δεν έχει πλεονέκτημα απέναντι στο άλλο. Στις περισσότερες περιπτώσεις οι προμηθευτές firewalls έχουν τροποποιήσει το λειτουργικό σύστημα, για να σκληραγωγηθεί και να το κάνουν πιο ανθεκτικό απέναντι στις επιθέσεις. Πρέπει να σημειώσουμε πως δεν είναι απαραίτητο για ένα δίκτυο που είναι αρχικά βασισμένο στα Windows να έχει ένα Windows firewall. Παρόλα αυτά είναι αναμφίβολα σημαντικό να επιλεγεί ένα τέτοιο σύστημα που ο διαχειριστής του θα νιώθει άνετα να διαχειριστεί.

- Χειρισμός Πρωτοκόλλων. Τα συστήματα firewalls αναπόφευκτα μένουν πίσω από την αιχμή της τεχνολογίας. Όλα τα firewalls θα χειριστούν FTP, ηλεκτρονικό ταχυδρομείο, HTTP, NNTP, TELNET και άλλα κοινά πρωτόκολλα, αλλά μπορεί να μην είναι ικανά να χειριστούν νέα ή ασυνήθιστα πρωτόκολλα όπως τα Pointcast, SNMP ή Real Audio. Αν επομένως απαιτείται να περάσετε ένα νέο πρωτόκολλο τηλεσυνδιάσκεψης μέσω του firewall πρέπει να έχετε σιγουρευτεί ότι το σύστημα μπορεί να το χειριστεί.
- Τύποι Φίλτρων. Τα φίλτρα δικτύου, που βασίζονται σε μεσολαβητές επιπέδου εφαρμογής, δίνουν εκτεταμένο έλεγχο σε οτιδήποτε περνά μέσω του firewall. Είναι επίσης, ικανά να αναλύσουν τα περιεχόμενα των δεδομένων και να τα τροποποιήσουν αν χρειάζεται. Το μειονέκτημα είναι, ότι αυτή η σε βάθος ανάλυση κουβαλά μια επιβάρυνση απόδοσης, η οποία μπορεί να είναι αξιοσημείωτη σε περιβάλλον που ήδη έχει βαριά κυκλοφορία δικτύου. Τα συστήματα που βασίζονται σε μεσολαβητές επιπέδου κυκλώματος έχουν καλύτερη απόδοση και τα συστήματα φιλτραρίσματος πακέτων ακόμη καλύτερη. Παρόλα αυτά και τα δύο συστήματα μπορούν να συντονίσουν συνδέσεις μόνο στη βάση των διευθύνσεων προορισμού και αποστολής, τις θύρες προορισμού και άλλους συντελεστές της TCP/IP επικεφαλίδας.
- Καταγραφή Ημερολογίου. Ένα καλό firewall πραγματοποιεί εξαντλητική καταγραφή ημερολογίου. Έρχεται επίσης με εργαλεία που αναλύουν και συνοψίζουν τα αρχεία του ημερολογίου έτσι ώστε να ανιχνεύσουν ασυνήθιστη δραστηριότητα.
- Διαχείριση. Τα περισσότερα firewalls παρέχουν ένα μηχανισμό απομακρυσμένης διαχείρισης αφού προηγουμένως πιστοποιήσουν προσεκτικά τον διαχειριστή.
- Απλότητα. Τα καλά συστήματα firewalls είναι απλά. Οι μεσολαβητές είναι μικροί, εύκολοι να κατανοηθούν και μπορούν να επαληθευτούν με επιθεώρηση. Κάποιες εταιρείες κάνουν ακόμη και τον πηγαίο κώδικα του συστήματός τους διαθέσιμο για δημόσια επιθεώρηση, ένα σημάδι της αυτοπεποίθησής τους στο λογισμικό τους.
- Διοχέτευση μέσω Κρυπτογραφικού καναλιού. Μερικά συστήματα firewalls παρέχουν την ικανότητα εγκατάστασης ενός κρυπτογραφικού καναλιού μέσω του διαδικτύου για να συνδεθούν με ασφάλεια δύο δίκτυα σε ένα απλό "εικονικό ιδιωτικό δίκτυο". Αυτός μπορεί να είναι ένας χρήσιμος τρόπος να συνδεθούν δύο γραφεία υποκαταστημάτων ή συνεργάτες και μπορεί να είναι πιο φθηνός από τον εναλλακτικό τρόπο της εκμίσθωσης μίας αφοσιωμένης γραμμής τηλεφώνου γι' αυτό το σκοπό.

Αδυναμίες των Συστημάτων Firewalls

Τα firewalls είναι γεγονός ότι προσφέρουν υψηλού επιπέδου προστασία απέναντι στους κινδύνους που προέρχονται από το διαδίκτυο. Υπάρχουν όμως και κίνδυνοι από τους οποίους τα firewalls αδυνατούν να μας προστατέψουν. Μερικές τέτοιες αδυναμίες τους είναι οι επόμενες:

- Το firewall δεν μπορεί να εμποδίσει τους εσωτερικούς κινδύνους. Μπορεί να έχει την δυνατότητα να ελέγχει τα δεδομένα που εισέρχονται και εξέρχονται του δικτύου δεν μπορεί όμως να εμποδίσει κάποιον από την εταιρεία (ή κάποιον που κατάφερε να μπει μέσα στα γραφεία της εταιρείας) να αντιγράψει δεδομένα σε δισκέττα, Cd, ή ακόμη και σε χαρτί και να τα μεταφέρει τελικά

εκτός της εταιρείας. Εάν ο εισβολέας βρεθεί πίσω και από το firewall τότε το firewall δεν μπορεί να τον ελέγξει, ούτε ασφαλώς να τον εμποδίσει.

- Δεν μπορεί να ελέγξει οτιδήποτε δεν περνάει από μέσα του. Το firewall παρακολουθεί και ελέγχει όλη την κίνηση που διέρχεται από μέσα του αλλά αδυνατεί να κάνει τα ίδια για τα δεδομένα εκείνα που δεν περνούν από το ίδιο.
- Δεν μπορεί να προστατέψει το σύστημα από νέες απειλές. Κανένα firewall δεν έχει τη δυνατότητα να ασφαλίσει το δίκτυο και τα δεδομένα, από καινούργιες απειλές. Η τοποθέτηση του δεν σημαίνει ότι το συγκεκριμένο σύστημα ασφαλείας εξασφαλίζει μόνιμη και διαρκή προστασία. Άλλωστε κανείς δεν μπορεί να γνωρίζει τι μορφή και τι δυνατότητες θα έχουν οι μελλοντικοί κίνδυνοι.
- Δεν μπορεί να προστατέψει το σύστημα από ιούς. Τα firewalls δεν είναι πλέον αποκλειστικό προνόμιο των εταιρικών δικτύων. Ο απλός χρήστης έχει αρκετές επιλογές για να εξασφαλίσει σε ένα μεγάλο βαθμό την ακεραιότητα του υπολογιστή του. Με την εγκατάσταση ενός Antivirus στον υπολογιστή σας, μειώνετε δραματικά την πιθανότητα εισβολής κάποιου ιού, σκουληκιού ή δούρειου ίππου. Με κανέναν όμως τρόπο δεν αποτρέπετε κακόβουλους hacker ή καλύτερα cracker από το να δοκιμάσουν να διεισδύσουν στον υπολογιστή σας χωρίς την έγκρισή σας. Για να εξασφαλιστείτε όσο το δυνατόν περισσότερο, θα πρέπει να εγκαταστήσετε στο PC σας κάποιο firewall. Θα πρέπει βέβαια να αναφέρουμε ότι δεν προσφέρουν απόλυτη προστασία.

Εάν, για παράδειγμα, το πανάκριβο firewall της Microsoft "τρύπησε", το ίδιο μπορεί να γίνει, αρκετά πιο εύκολα μάλιστα, και στα PC μας. Βέβαια, η Microsoft και κάθε άλλος εταιρικός δικτυακός τόπος είναι επώνυμοι στόχοι και είναι φυσικό να προσελκύουν το ενδιαφέρον των απανταχού cracker, ενώ ο απλός χρήστης είναι στην κυριολεξία σταγόνα μέσα στον ωκεανό. Παρ' όλα αυτά, υπάρχουν δυστυχώς αρκετοί ερασιτέχνες και ημιεπαγγελματίες οι οποίοι "σκανάρουν" το Internet για να βρουν "ανοιχτές πόρτες" στους υπολογιστές μας. Εάν κάποιος έχει μόνιμη σύνδεση με το Internet (και κατά συνέπεια σταθερό IP), εάν λειτουργεί κάποιο διακομιστή (π.χ., Web) στον υπολογιστή σας ή εφαρμογή απομακρυσμένης πρόσβασης (PC Anywhere-Wingate κ.λπ.) ή απλώς επιθυμεί να ελέγχει τι εισέρχεται και τι «φεύγει» από το PC του, θα πρέπει να εγκαταστήσει ένα firewall. Μόνο έτσι θα απομονωθεί το σύστημά από το Internet και στην ουσία θα "εξαφανιστεί" από τον έξω κόσμο, ακόμα και αν είναι on-line.

Επιπλέον, με βάση κάποιους συγκεκριμένους κανόνες, ελέγχει και κατά συνέπεια επιτρέπει ή εμποδίζει να εισέλθουν στον υπολογιστή ή να εξέλθουν από αυτόν τα πακέτα δεδομένων του Internet.

3.2 Προστασία Οικονομικών Συναλλαγών με την Μέθοδο των Passwords

Τα passwords είναι η πιο συνηθισμένη διαδικασία που χρησιμοποιείται σχεδόν παντού για να διασφαλίζει και να επιβεβαιώνει την ταυτότητα του χρήστη, επιτρέποντάς του εν συνεχεία την είσοδο στο κάθε σύστημα. Η συγκεκριμένη μέθοδος εφαρμόζεται για κάθε είσοδο χρήστη σε ένα πληροφοριακό σύστημα ή στο δίκτυο. Από το χρήστη ζητούνται το user name και το password του, τα οποία εφόσον ταιριάζουν με αυτά που υπάρχουν στο password file, θεωρούνται από το σύστημα ως επιβεβαίωση της ταυτότητάς του και έτσι ο χρήστης εισάγεται εντός του συστήματος ή του δικτύου. Τα passwords θεωρούνται ως αξιόπιστη και ασφαλής διαδικασία

ελέγχου ταυτότητας αλλά όπως σε όλα τα θέματα που αφορούν την ασφάλεια έτσι και εδώ ο κίνδυνος κρύβεται στις λεπτομέρειες και οι οποίες αναφέρονται ως εξής:

- 1ος Κίνδυνος

Η επιλογή του password είναι ίσως το κρισιμότερο σημείο και αυτό διότι οι επιλογές που κάνουν οι χρήστες συνήθως είναι προβλέψιμες. Αν από την άλλη τους δοθεί έτοιμο το password τότε επιλέγουν να το σημειώσουν παρά να το αποστηθίσουν. Στη χειρότερη περίπτωση θα ανακαλύψει κάποιος το password σε σημείωμα κολλημένο στο πλάι της οθόνης του υπολογιστή του χρήστη. Η ορθότερη επιλογή είναι το password να αποτελείται από συνδυασμό γραμμάτων και αριθμών.

- 2ος Κίνδυνος

Προκειμένου τα passwords να εξασφαλίζουν προστασία πρέπει τακτικά να αντικαθίστανται από νέες επιλογές. Οι χρήστες δυστυχώς αποφεύγουν αυτή την αλλαγή ή επιλέγουν να ανακυκλώνουν ένα μικρό αριθμό από passwords. Καλό θα ήταν η τακτική αλλαγή τους να επιβάλλεται από το ίδιο το λογισμικό.

- 3ος Κίνδυνος

Εάν κάποιος έχει λογαριασμούς σε διαφορετικούς υπολογιστές ή sites στο internet θα πρέπει για λόγους ασφαλείας να χρησιμοποιεί διαφορετικά passwords για την είσοδό του σε κάθε σύστημα ή ιστοσελίδα. Ασφαλώς, κάτι τέτοιο είναι ιδιαίτερα δύσκολο για τον χρήστη και το πιθανότερο είναι κάπου να τα σημειώσει προκειμένου να μην τα ξεχάσει. Από την άλλη μεριά η ύπαρξη ενός μόνο password αυξάνει την πιθανότητα από κάπου να αποκαλυφθεί. Σε κάθε περίπτωση η όσο το δυνατόν συχνότερη αντικατάστασή τους είναι μια καλή και ενδεδειγμένη πρόταση.

- 4ος Κίνδυνος

Είναι προφανές πως το σημείο που το σύστημα ή το δίκτυο αποθηκεύει τα διάφορα passwords είναι σημείο που απαιτεί αυξημένη ασφάλεια αφού αποτελεί βασικό στόχο για εισβολή. Ο συνηθισμένος τρόπος για να περιορίζεται ο κίνδυνος είναι να μην αποθηκεύονται ως κείμενο, ούτε ακόμη και με κρυπτογράφηση (encrypted), αλλά με τη μορφή που έχει το καθένα ως συνάρτηση hash. Η αντιστροφή της τιμής της συνάρτησης στο αντίστοιχο password είναι εξαιρετικά δύσκολη και έτσι τα passwords, ναι μεν δεν μπορούν να ανακτηθούν, αλλά εύκολα μπορεί να γίνεται ο έλεγχος ανάμεσα στο αποθηκευμένο password και σε αυτό που πληκτρολογείται κατά την είσοδο ενός χρήστη.

Στις μεθόδους για επιβεβαίωση της ταυτότητας κάποιου χρήστη εκτός από τα passwords, συμπεριλαμβάνονται ακόμη:

- Passwords μιας χρήσης

Ένα πρόβλημα που αντιμετωπίζει η τεχνολογία των passwords είναι πως αν μεταδοθεί από μη ασφαλές τηλεπικοινωνιακό κανάλι τότε αυξάνεται αισθητά ο κίνδυνος να έχει υποκλαπεί. Μία λύση στο πρόβλημα είναι ο κάθε χρήστης να έχει ένα σύνολο από passwords που το καθένα θα μπορεί να χρησιμοποιηθεί μόνο μια φορά. Ένα τέτοιο σύστημα είναι το S/Key το οποίο χρησιμοποιεί μία συνάρτηση η οποία παράγει την αλυσίδα των διαδοχικών password. Στην πράξη κάθε έγκυρο password αντικαθίσταται στη συνάρτηση και έτσι σχηματίζεται το επόμενο.

- Smart Cards

Όπως έχουμε πει και στο προηγούμενο κεφάλαιο, πρόκειται για μικρές κάρτες - αντίστοιχες με τις πιστωτικές- οι οποίες περιέχουν έναν επεξεργαστή, κάποια μνήμη και μια διασύνδεση με το εξωτερικό περιβάλλον. Χρησιμοποιούνται σε μία σειρά εφαρμογών συμπεριλαμβάνοντας και την ηλεκτρονική πληρωμή. Εκτελούν τρεις βασικές λειτουργίες: Αποθήκευση και διαχείριση πληροφοριών, επιβεβαίωση της ταυτότητας του χρήστη, καθώς και κρυπτογράφηση-αποκρυπτογράφηση. Το πλεονέκτημά της ως προς την ασφάλεια είναι ότι λειτουργεί σε ένα απομονωμένο περιβάλλον. Σήμερα, υπάρχει μία μεγάλη γκάμα από smart cards, οι οποίες μεταξύ τους διαφέρουν στην απόδοση και την ικανότητα του επεξεργαστή, το μέγεθος της μνήμης καθώς και την ταχύτητα διασύνδεσης με το εξωτερικό περιβάλλον. Για να λειτουργήσει απαιτείται η ύπαρξη της συσκευής που θα "διαβάσει" την smart card. Υπάρχουν διαφόρων ειδών τέτοιες συσκευές ανάλογα με τι είδους τεχνολογία διαθέτουν. Έτσι υπάρχουν συσκευές που διαβάζουν την smart card όταν αυτή τοποθετηθεί στην ειδική σχισμή και άλλες που είναι χωρίς επαφή και τη "διαβάζουν" με τη βοήθεια υπέρυθρων ακτινών.
Είτε με την πρώτη, είτε με τη δεύτερη μέθοδο, επιτυγχάνεται η απαραίτητη ανταλλαγή δεδομένων ανάμεσα σε κάρτα και συσκευή ανάγνωσης και έτσι γίνεται ο έλεγχος της ταυτότητας του χρήστη.

- Antivirus

Παρά την ύπαρξη περίπου πενήντα χιλιάδων ιών, σύμφωνα με το Norton Antivirus (προφανώς πρέπει να είναι ιδιαίτερα διασκεδαστικός ο σχεδιασμός τους, ώστε να δικαιολογείται το πλήθος τους), εάν τηρηθούν μερικοί βασικοί κανόνες, ελαχιστοποιείται ο κίνδυνος μόλυνσης. Εκτός από την αναβάθμιση των εφαρμογών που σχετίζονται με το Internet, είναι πλέον επιβεβλημένη η εγκατάσταση στο πληροφοριακό σύστημα κάποιας εφαρμογής προστασίας από τους ιούς. Μετά την εγκατάσταση θα πρέπει να γίνεται εβδομαδιαία ενημέρωση από τους δημιουργούς του antivirus (μέσω Internet κατά προτίμηση), ώστε να υπάρχει αυξημένο επίπεδο προστασίας απέναντι και στους νεότερους των ιών.
Με την τεράστια εξάπλωση των ιών και των σκουληκιών που χρησιμοποιούν κυρίως το e-mail για να εξαπλωθούν, το antivirus να είναι ικανό να ελέγχει και την εισερχόμενη αλληλογραφία της εταιρείας, προστατεύοντας έτσι το σύστημα από τον βασικότερο τρόπο εγκατάστασης των ιών από το εξωτερικό περιβάλλον. Με αυτό τον τρόπο συλλαμβάνονται τα κακόβουλα προγράμματα, προτού φτάσουν στο ηλεκτρονικό γραμματοκιβώτιο της εταιρείας.

Βέβαια, οι εφαρμογές προστασίας δεν λειτουργούν πάντα καλά, με συνέπεια να παρουσιάζονται περιστασιακά προβλήματα στη λήψη της αλληλογραφίας, αλλά μπροστά στον υπαρκτό κίνδυνο, τα συγκεκριμένα προβλήματα είναι αποδεκτά. Γενικά, δεν πρέπει να εκτελούνται επισυναπτόμενα αρχεία, εάν δεν υπάρχει βεβαιότητα για την καθαρότητά τους. Ακόμα και αν φαίνονται αθώα (μια εικόνα jpg, για παράδειγμα) ή προέρχονται από γνωστό αποστολέα, δεν αποκλείεται το αρχείο να είναι εκτελέσιμο και να έχει τη μορφή picture.jpg.exe (όπως, π.χ., συμβαίνει σε έναν πρόσφατο δούρειο ίππο του ICQ).

Υπάρχουν ελάχιστες είναι οι πιθανότητες να μολυνθεί το σύστημα ανοίγοντας απλώς ένα e-mail. Θα πρέπει να εκτελεστεί ο επισυναπτόμενος, καμουφλαρισμένος, κακόβουλος κώδικας. Προσοχή χρειάζεται και με τα αρχεία word και excel που λαμβάνονται, τα οποία καλό θα είναι να περνούν από έλεγχο για μακροϊούς. Επίσης,

πρέπει να προσεχθούν και οι διάφορες εφαρμογές που εγκαθίστανται, ειδικά εάν προέρχονται από αμφιλεγόμενες πηγές. Η παρουσία του antivirus προστατεύει επίσης το σύστημα και από τους εσωτερικούς κινδύνους για την περίπτωση που κάποιος χρήστης είτε εν αγνοία του, είτε εσκεμμένα προσπαθήσει να εγκαταστήσει έναν τέτοιο ιό. Άλλωστε ο κίνδυνος των δολιοφθορών εκ των έσω πρέπει να βρίσκεται ιδιαίτερα ψηλά στην ιεραρχία των κινδύνων, για το σχεδιαστή του συστήματος ασφαλείας.

Όλα τα παραπάνω είναι πολύ καλά για την πρόληψη. Τι πρέπει να γίνεται όμως στην περίπτωση που το πληροφοριακό σύστημα μολυνθεί από κάποιον ιό; Αυτό είναι κάτι που διαπιστώνεται με την παρατήρηση βασικών χαρακτηριστικών και συμπεριφορών του υπολογιστή. Εάν ξαφνικά αρχεία εμφανίζονται ή εξαφανίζονται, το σύστημα γίνεται πιο αργό, μειώνεται η διαθέσιμη μνήμη, εφαρμογές αρνούνται να τρέξουν ή παράξενα μηνύματα εμφανίζονται στην οθόνη, όλα αυτά είναι ενδείξεις που "φωτογραφίζουν" την παρουσία ιού. Η αμέσως επόμενη κίνηση είναι να ελεγχθεί ο υπολογιστής με κάποιο antivirus.

Αφού εντοπιστεί ο ιός και καθαρίσει το σύστημα, καλό θα ήταν να δημιουργηθούν δισκέτες ασφαλείας, διαδικασία η οποία συνήθως προσφέρεται από το antivirus πρόγραμμα που χρησιμοποιείται από το σύστημα. Οι δισκέτες αυτές δίνουν τη δυνατότητα να εκκινηθεί το σύστημα και να γίνει έλεγχος για ιούς, ενώ μπορεί να περιέχουν και αντίγραφα των τομέων εκκίνησης του σκληρού δίσκου σε περίπτωση μόλυνσης του boot sector.

3.3 Εχθροί και Τρόποι Άμυνας στην Κρυπτογράφηση των Οικονομικών Συναλλαγών

Βασικό τμήμα του σχεδιασμού ενός συστήματος ασφαλείας οικονομικών συναλλαγών, αποτελεί να εξακριβώσουμε τι επίπεδο ασφάλειας χρειάζεται και ποιές απειλές θα κληθεί να αντιμετωπίσει. Η επιλογή των μέτρων προστασίας γίνεται λαμβάνοντας υπόψη τι κόστος (οικονομικό, απόδοσης ή ενόχλησης λόγω της παρουσίας τους) έχουν για την εταιρεία. Το πρώτο λοιπόν, βήμα είναι να εντοπιστεί ο εχθρός. Συνήθως οι άνθρωποι επικεντρώνονται στο είδος της επίθεσης ξεχνώντας ότι οι επιθέσεις είναι τα εργαλεία. Για παράδειγμα, ένας αποφασισμένος εισβολέας θα επιμείνει πολύ περισσότερο από ένα τυπικό εισβολέα. Έτσι, παρόλο που θα χρησιμοποιηθούν τα ίδια είδη επίθεσης, η επιμονή μπορεί να είναι αυτή που θα αποβεί καταλυτική για την επιτυχία ή μη της επίθεσης. Για το λόγο αυτό είναι σημαντικό να έχουν προσδιοριστεί πρώτα:

- Ποιοί είναι οι εχθροί.
- Ποιές είναι οι προθέσεις τους.
- Ποιά είναι τα μέσα τους

Οι εχθροί των Πληροφοριακών Συστημάτων

Οι εν δυνάμει εχθροί ενός πληροφοριακού συστήματος οικονομικών συναλλαγών κατηγοριοποιούνται στις ακόλουθες ομάδες:

- Hackers – Crackers. Είναι οι "αναρχικοί" του κυβερνοχώρου που εισβάλουν στα πληροφοριακά συστήματα είτε για διασκέδαση, είτε για να καταστρέψουν, είτε για επίδειξη. Τους ελκύουν όλοι οι απαγορευμένοι χώροι. Πολλές εταιρείες συνηθίζουν να προσλαμβάνουν άτομα που εισέβαλαν στα συστήματά τους με τη λογική "Καλύτερα να δουλεύουν για μας παρά εναντίον μας". Άλλωστε αυτοί που παραβίασαν ένα σύστημα ασφαλείας ξέρουν καλύτερα από τον καθένα που μειονεκτεί και μπορούν να το βελτιώσουν.

- Κλέφτες. Είναι όλοι αυτοί που εισβάλουν σε ένα σύστημα έχοντας ως στόχο την κλοπή δεδομένων που θα τους αποφέρει οικονομικά οφέλη είτε χρησιμοποιώντας τα, είτε πουλώντας τα.

- Ανταγωνιστές. Ένας ανταγωνιστής συνήθως, δεν εισβάλει για να κλέψει χρήματα, ούτε για να καταστρέψει αλλά για να αποκτήσει πληροφορίες που είναι σημαντικές προκειμένου να κυριαρχήσει στον "επιχειρηματικό πόλεμο".

- Εσωτερικοί εχθροί. Δυσαρεστημένοι, αποξενωμένοι και άπληστοι υπάλληλοι μπορούν να αποτελέσουν ένα ιδιαίτερα σοβαρό εκ των έσω κίνδυνο για τις βάσεις δεδομένων μιας εταιρείας.

- Ατυχήματα. Πολλές καταστροφές δεν είναι αποτέλεσμα πρόθεσης ούτε οργανωμένης επίθεσης, αλλά πρόκειται για ατυχήματα ή λάθη από αφέλεια. Δεν είναι καθόλου ασυνήθιστο γεγονός εταιρείες να καταστρέφουν από μόνες τους τις βάσεις δεδομένων τους, ή να τις απελευθερώνουν στο internet κατά λάθος. Έχοντας γνωρίσει τους πιθανούς εισβολείς ενός συστήματος, εν συνεχεία, περιγράφονται οι τρόποι που έχουν οι crackers για να αποκτούν παράνομη ή έστω παράτυπη πρόσβαση σε υπολογιστικά συστήματα, τα εργαλεία που χρησιμοποιούν για να κερδίζουν τον έλεγχο σε υπολογιστές, καθώς και τις διαθέσιμες τεχνικές στις οποίες καταφεύγουν για να προκαλούν ζημιές ή να «γονατίζουν» ένα σύστημα, ανεξαρτήτως της ισχύος του.

3.4 Τύποι Επιθέσεων

Μία από τις πλέον διάσημες και αποτελεσματικές μεθόδους που χρησιμοποιούν οι crackers για να θέτουν εκτός λειτουργίας δικτυωμένους υπολογιστές ενός συστήματος ασφαλείας οικονομικών συναλλαγών είναι οι επιθέσεις DoS (Denial of Service attacks). Το όνομα της τεχνικής (άρνηση εξυπηρέτησης) οφείλεται στο γεγονός ότι ο υπολογιστής-θύμα για ένα χρονικό διάστημα δεν είναι σε θέση να εξυπηρετεί αιτήσεις μηχανημάτων-πελατών (clients), εξαιτίας του τεράστιου πλήθους κίβδηλων αιτήσεων (bogus requests) που δέχεται από τον επιτιθέμενο.
Υπάρχουν διάφορα είδη επιθέσεων DoS, πολλά από τα οποία εκμεταλλεύονται εγγενείς αδυναμίες του ζεύγους πρωτοκόλλων TCP/IP. Για τα περισσότερα από αυτά είναι ήδη γνωστά τα αντίστοιχα μέτρα προστασίας. Συγκεκριμένα, οι διαχειριστές συστημάτων μπορούν να εγκαθιστούν patches σε λειτουργικά συστήματα και προγράμματα - διακομιστές, ώστε να αποτρέπουν επιθέσεις DoS ή να ελαχιστοποιούν τις συνέπειές τους. Όπως, όμως, συμβαίνει και με τους ιούς υπολογιστών, κατά καιρούς εφευρίσκονται νέα είδη ή παραλλαγές επιθέσεων DoS.

Παρακάτω παραθέτονται εν συντομία τέσσερις από τις διασημότερες παραλλαγές.

- Ping of death. Αίτηση PING ή, αλλιώς, αίτηση ICMP, προς τον υπολογιστή-στόχο, με άκυρο μέγεθος πακέτου στην κεφαλή (header) του τελευταίου (πάνω από 64Kb). Τέτοια «παράτυπα» πακέτα μπορούν να «κρεμάσουν» υπολογιστές που τρέχουν λειτουργικά συστήματα ανίκανα να τα μεταχειριστούν.

- Smurf Attack. Επιτυγχάνεται αποστέλλοντας αιτήσεις ICMP σε μια διεύθυνση εκπομπής (broadcast address) στο υπό επίθεση δίκτυο ή σε κάποιο άλλο, ενδιάμεσο. Η διεύθυνση επιστροφής (return address) των πακέτων ICMP πλαστογραφείται, ώστε να είναι ίδια με αυτήν του υπολογιστή-στόχου. Από τη στιγμή που μια διεύθυνση εκπομπής αντιστοιχεί σε όλα τα μηχανήματα ενός υποδικτύου, λειτουργεί ενισχυτικά, δημιουργώντας από μία μόνο αίτηση ICMP δεκάδες ή και εκατοντάδες απαντήσεις, προκαλώντας με τον τρόπο αυτό πληροφοριακό «μποτιλιάρισμα».

Ας σημειωθεί ότι μια διεύθυνση εκπομπής αντιστοιχεί το πολύ σε 255 μηχανήματα (ανήκουν όλα στο ίδιο υποδίκτυο), επομένως κατά τη διάρκεια μιας επίθεσης Smurf, από κάθε αίτηση PING μπορούν να παραχθούν μέχρι και 255 απαντήσεις. Γίνεται κατανοητό, λοιπόν, ότι από τον υπέρογκο αριθμό των άχρηστων πακέτων που δημιουργούνται, ο επιτιθέμενος μπορεί να στέλνει εκατοντάδες ή ακόμη και χιλιάδες πακέτα ICMP.

- Syn flood attack. Πριν εγκαθιδρυθεί μια συνεδρία μεταξύ ενός πελάτη και ενός διακομιστή, λαμβάνει χώρα μια ακολουθία τριών βημάτων, γνωστή και ως «ακολουθία χειραψίας» (handshaking sequence). Εάν ο πελάτης αγνοήσει την τελευταία απάντηση SYN-ACK (SYNchronize ACKnowledge) του διακομιστή, ο τελευταίος θα επιμένει για ένα προκαθορισμένο χρονικό διάστημα. Ένας cracker μπορεί να εκμεταλλευτεί τη συγκεκριμένη συμπεριφορά για να υπερφορτώσει το διακομιστή-θύμα ή ακόμα και για να τον «κρεμάσει». Κατά τη διάρκεια μιας τέτοιας επίθεσης, ο θύτης παραποιεί τη δικτυακή του διεύθυνση (IP address), κρύβοντας με τον τρόπο αυτό τα ίχνη του.

- Tear Drop Attack. Ο επιτιθέμενος εκμεταλλεύεται αδυναμίες στην ανασυγκρότηση των πακέτων IP. Όταν ένα τέτοιο πακέτο αποστέλλεται στο Internet, ενδέχεται να ταξιδεύει σε επιμέρους, μικρότερα τμήματα. Κάθε τμήμα περιλαμβάνει στην κεφαλή του ένα πεδίο, όπου εκεί περιγράφεται η θέση του στο αρχικό πακέτο IP. Ο θύτης χρησιμοποιεί ένα πρόγραμμα, ονόματι «Teardrop», το οποίο τεμαχίζει πακέτα IP σε τμήματα με λανθασμένες πληροφορίες στο υπό συζήτηση πεδίο. Όταν ο υπολογιστής-στόχος προσπαθήσει να συναρμολογήσει τα «παραπλανητικά» αυτά τμήματα, θα κολλήσει ή θα επανεκκινήσει, εκτός και αν ο διαχειριστής συστήματος έχει φροντίσει να αναβαθμίσει το λειτουργικό με το κατάλληλο patch που διορθώνει το πρόβλημα.

Όταν σε μια επίθεση DoS συμμετέχουν περισσότερα του ενός μηχανήματα, έχουμε τις λεγόμενες κατανεμημένες επιθέσεις DoS (Distributed Denial of Service ή DDoS attacks). Στις επιθέσεις του είδους είναι δυνατόν να συμμετέχουν και προσωπικοί υπολογιστές ακόμα και το PC που βρίσκετα στο σπίτι χωρίς να το γνωρίζουν οι χρήστες τους. Ο επιτιθέμενος cracker κατορθώνει με κάποιον τρόπο να βάλει ένα μικρό πρόγραμμα σε καθένα από τα μηχανήματα που θα συμμετάσχουν εν αγνοία τους στην επίθεση.

Τη στιγμή που θα την εξαπολύσει, στέλνει μια ειδοποίηση σε ένα από αυτά (διακομιστής DDoS). Τότε, εκείνο ειδοποιεί μια συγκεκριμένη χρονική στιγμή καθέναν από τους υπόλοιπους υπολογιστές (πελάτες DDoS) και όλοι μαζί αρχίζουν να βάλλουν κατά του στόχου με πλαστές αιτήσεις. Το αποτέλεσμα είναι εκείνος να «πλημμυρίσει» και να μην μπορεί να ανταποκριθεί σε αιτήσεις νομότυπων πελατών. Ένας καλός τρόπος για να προστατευτούν οι υπολογιστές, ώστε να μη χρησιμοποιούνται χωρίς τη θέληση του κατόχου, είναι να χρησιμοποιείται κάποιο προσωπικό πρόγραμμα firewall.

Αν και ένα μηχάνημα που έχει πέσει θύμα επίθεσης DoS ή DDoS μπορεί να επανέλθει σε ομαλή λειτουργία σχετικά εύκολα, υπάρχουν έμμεσες αρνητικές συνέπειες. Οι οικονομικές ζημιές που οφείλονται στο χρόνο που ένας κεντρικός διακομιστής μένει εξουδετερωμένος, καθώς και στον τραυματισμό του κύρους της εταιρείας στην οποία ανήκει ο διακομιστής-θύμα. Είναι γνωστό, εξάλλου, ότι στην διαδικτυακή εποχή ο ανταγωνισμός βρίσκεται μερικά «κλικ» μακρύτερα.

- Απρόσκλητοι Ωτακουστές. Από τα παλαιότερα εργαλεία που χρησιμοποιούσαν και συνεχίζουν να χρησιμοποιούν οι διαχειριστές συστημάτων για να αναλύουν τη συμπεριφορά δικτύων και να εντοπίζουν (πιθανά) προβλήματα, είναι τα λεγόμενα «sniffer». Έτσι ονομάζεται ένα πρόγραμμα που είναι ικανό να «υποκλέπτει» δεδομένα που ταξιδεύουν σε ένα δίκτυο. Εάν το δίκτυο είναι βασισμένο στο TCP/IP, τότε επειδή το sniffer παρακολουθεί πακέτα IP, ονομάζεται και packet sniffer. Εξάλλου, σε ένα δίκτυο τοπολογίας αστέρα, όπως είναι πολλά τοπικά δίκτυα, τα πακέτα που φεύγουν από έναν κόμβο (μηχάνημα) εκπέμπονται προς όλους τους άλλους κόμβους του δικτύου. Ωστόσο, μόνο ο κόμβος για τον οποίο προορίζονται τα πακέτα θα τα χρησιμοποιήσει, οι άλλοι θα τα αγνοήσουν. Εάν, τώρα, ένα πρόγραμμα sniffer είναι εγκατεστημένο σε έναν υπολογιστή με κάρτα δικτύου σε «επιδιδόμενη» κατάσταση (promiscuous mode), τότε το μηχάνημα αυτό θα μπορεί να «βλέπει» όλα τα πακέτα που διακινούνται στο δίκτυο.

Οι διαχειριστές συστημάτων κάνουν χρήση των sniffer για να αναλύουν την κυκλοφορία των πακέτων σε ένα δίκτυο και να εντοπίζουν εστίες προβλημάτων. Επίσης, συχνά χρησιμοποιούν περισσότερα του ενός sniffer, στρατηγικά εγκατεστημένα σε διάφορους κόμβους του δικτύου, ώστε να εντοπίζουν εισβολές παρείσακτων. Με άλλα λόγια, τα sniffer μπορούν να λειτουργήσουν και ως ένα σύστημα ανίχνευσης εισβολών (intrusion detection systems). Είναι φανερό λοιπόν ότι τα προγράμματα αυτά αποτελούν πολύτιμο εργαλείο για τους διαχειριστές συστημάτων. Ωστόσο, όπως ήδη θα έχει γίνει προφανές, τις υπηρεσίες τους μπορούν να εκμεταλλευτούν και οι crackers, αυτή τη φορά για όχι και τόσο θεάρεστους σκοπούς. Για παράδειγμα, ο cracker μπορεί να χρησιμοποιεί ένα sniffer για να υποκλέπτει κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών, διάφορα άλλα

προσωπικά στοιχεία χρηστών, για να διαβάζει την ηλεκτρονική τους αλληλογραφία κ.λπ..

Ο προφανής τρόπος για να προστατευτεί ένα δίκτυο από την επιβλαβή χρήση των sniffer είναι να υπάρχει αυστηρή επίβλεψη στα προγράμματα που εγκαθιστούν οι χρήστες στους υπολογιστές. Εάν ένας cracker δεν μπορεί να αποκτήσει φυσική πρόσβαση σε κάποιον υπολογιστή, τότε είναι απλώς ανίκανος να εγκαταστήσει ένα sniffer. Άλλος ένας τρόπος για την παρόπλιση των sniffer είναι η αποστολή δεδομένων σε κρυπτογραφημένη μορφή. Το sniffer θα εξακολουθεί να συλλαμβάνει τα πακέτα, μόνο που τώρα δεν θα μπορεί να εξαγάγει κάποιο νόημα από τα περιεχόμενά τους. Βεβαίως, στην περίπτωση αυτή υπάρχει πάντοτε ο κίνδυνος της αποκρυπτογράφησης. Για το λόγο αυτό, προτείνεται η χρήση ισχυρής κρυπτογραφίας, με το ανάλογο κόστος σε υπολογιστική ισχύ. Το ζητούμενο, λοιπόν, είναι η χρυσή τομή ανάμεσα στη δύναμη των μεθόδων κρυπτογράφησης από τη μία, και στην ευκολία των χρηστών, από την άλλη.

Τέλος, υπάρχει μια ολόκληρη κατηγορία προγραμμάτων που μπορούν να εντοπίζουν ποιοι υπολογιστές σε ένα δίκτυο έχουν κάρτα δικτύου σε επιδιδόμενη κατάσταση. Έτσι, ο διαχειριστής συστήματος μπορεί να ελέγξει εάν κάποιος υπολογιστής τρέχει ένα sniffer, αν έχει δοθεί επίσημη άδεια για την εγκατάστασή του κ.λπ..

- Αδιάκριτοι Διαβάτες. Μια άλλη τεχνική που χρησιμοποιούν διαχειριστές και crackers, καθένας για διαφορετικούς σκοπούς, είναι η σάρωση θυρών (port scanning). Πρόκειται για μια διαδικασία αποστολής ερωτημάτων σε διακομιστές, με σκοπό να ληφθούν πληροφορίες για τις υπηρεσίες που προσφέρουν, καθώς και για το χρησιμοποιούμενο επίπεδο ασφαλείας. Από τη στιγμή που ο επίδοξος εισβολέας μάθει ποιες υπηρεσίες προσφέρει το μηχάνημα-στόχος, μπορεί στη συνέχεια να σχεδιάσει την επίθεσή του βασιζόμενος σε γνωστές αδυναμίες των υπηρεσιών. Επειδή μια διαδικασία port scanning αφήνει τα ίχνη της στα αρχεία καταγραφής (log files) του λειτουργικού συστήματος, ορισμένοι crackers χρησιμοποιούν ορισμένες «ύπουλες» παραλλαγές. Μία από αυτές είναι η λεγόμενη «ημι-ανοιχτή σάρωση SYN» (half-open SYN scan). Κατά τη διάρκεια μιας τέτοιας σάρωσης, το πρόγραμμα συνδέεται στα port, αλλά τερματίζει καθεμία ακολουθία σύνδεσης, πριν αυτή ολοκληρωθεί. Από τη στιγμή, λοιπόν, που οι ακολουθίες σύνδεσης δεν ολοκληρώνονται, το λειτουργικό σύστημα στο μηχάνημα-στόχος συνήθως δεν τις καταγράφει, θεωρώντας ότι δεν συνέβησαν ποτέ. Ωστόσο, το πρόγραμμα που κάνει τη σάρωση μπορεί να καταλάβει εάν κάποιο port είναι «ανοιχτό», κρίνοντας από την απάντηση του λειτουργικού συστήματος. Υπάρχουν διάφορα εργαλεία για το μπλοκάρισμα των port scan. Αυτό που προτείνεται στους απλούς χρήστες είναι η χρήση κάποιου προσωπικού προγράμματος firewall.

- Social Engineering. Ακούγεται ειρωνικό αλλά αποτελεί μια πραγματικότητα, το γεγονός ότι μία από τις πιο ύπουλες μεθόδους επίθεσης σε ένα σύστημα ασφαλείας δεν βασίζεται στην τεχνολογία αλλά στην ψυχολογία! Ως "social engineering" ορίζεται η "τέχνη" της πρόσβασης σε ένα σύστημα, εξαπατώντας τους χρήστες και τους διαχειριστές του και αποσπώντας τους όλες εκείνες τις πληροφορίες που χρειάζονται. Σε ένα πείραμα που έγινε, μια ομάδα από hackers ξεκίνησαν την προσπάθειά τους να διεισδύσουν σε ένα πληροφοριακό σύστημα μεγάλης εταιρείας. Μοναδικό τους όπλο είχαν τον τηλεφωνικό

κατάλογο της εταιρείας. Τηλεφώνησαν στην εταιρεία, ζήτησαν να μιλήσουν με το γραμματεία του δικτύου και κατόρθωσαν μέσα σε εικοσιτέσσερις ώρες η ίδια η εταιρεία να τους δημιουργήσει λογαριασμό, να τους δώσει ID και κωδικό μέσω τηλεφώνου και μάλιστα να τους στείλει με courier μέσα στη νύχτα το απαιτούμενο, για την είσοδό τους στο δίκτυο, software.

- Ιοί. Αναμφίβολα το Internet έδωσε μεγάλη ώθηση στην εξάπλωση των πάσης φύσεως ιών και «μικροβίων». Στις μέρες της Amiga και των PC XT ο μόνος τρόπος για να «κολλήσει» κάποιος ένα ειδεχθές πρόγραμμα ήταν να χρησιμοποιήσει μολυσμένες δισκέτες, κυρίως με παιχνίδια. Τότε η μόλυνση με έναν ιό ήταν κάτι το συνηθισμένο μέχρι και γοητευτικό (το γνωστό μπαλάκι που έκανε βόλτες στην οθόνη). Βέβαια, το αστείο τελείωνε με την οδυνηρή ανακάλυψη ότι οι δισκέτες ή ο σκληρός δίσκος ήταν άχρηστα. Η κατάσταση άλλαξε δραματικά με την είσοδο του Internet στη ζωή μας, και συγκεκριμένα με το e-mail. Το ηλεκτρονικό ταχυδρομείο εκμηδένισε τις αποστάσεις και έκανε την επικοινωνία ανάμεσα στους εταιρικούς και τους οικιακούς χρήστες πολύ εύκολη και ευχάριστη υπόθεση. Το e¬mail όμως είναι προς το παρόν το κυριότερο μέσο για τη μετάδοση κάθε είδους ιών και σκουληκιών, μετατρέποντάς τα σε πραγματική επιδημία λόγω της μεγάλης ταχύτητας με την οποία εξαπλώνονται. Στη συντριπτική τους πλειονότητα οι ιοί, τα σκουλήκια και οι δούρειοι ίπποι δεν μπορούν να προκαλέσουν καμία ζημιά, εάν δεν τρέξετε τα εκτελέσιμα αρχεία/script που τα μεταφέρουν. Η κακόβουλη αυτή εφαρμογή μπορεί να έχει καλυφθεί κάτω από το μανδύα μιας εικόνας ή ενός κειμένου word, παραπλανώντας σας ή κάνοντας πολύ δύσκολο τον εντοπισμό της από το χρήστη. Με τον όρο ιοί, ορίζονται κατά κύριο λόγο τα προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή χωρίς την έγκρισή μας και να μολύνουν άλλα αρχεία. Είναι μικρά κομμάτια ηλεκτρονικού κώδικα, που έχουν τη δυνατότητα να αντιγράφουν και να εισάγουν τον εαυτό τους σε ένα εκτελέσιμο πρόγραμμα, αρχείο, δισκέτα ή μέρος σκληρού δίσκου. Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι μηδαμινές έως και καταστροφικές. Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο το δυνατόν περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο Internet. Υπάρχουν αρκετά ήδη ιών:

- Αυτοί που προσβάλλουν τον τομέα εκκίνησης μιας δισκέτας ή ενός σκληρού δίσκου (boot sector viruses) και είναι σχετικά σπάνιοι σήμερα

- Αυτοί που περιέχονται σε εκτελέσιμα αρχεία (Program/File viruses)

- Αυτοί που εκμεταλλεύονται τις γλώσσες μακροεντολών, όπως, π.χ., του Word και του Excel (Macro viruses)

- Οι πολυμορφικοί, οι οποίοι μπορεί να ανήκουν σε μερικές ή όλες τις προαναφερθείσες κατηγορίες.

- Υπάρχει και μία ειδική κατηγορία ιών, η οποία εκμεταλλεύεται αδυναμίες γνωστών εφαρμογών, όπως, για παράδειγμα, το Outlook Express, με αποτέλεσμα ένα απλό e-mail κειμένου να μπορεί να κάνει τη ζημιά.

Βέβαια, οι ιοί αυτοί είναι σπάνιοι και παροπλίζονται με την εγκατάσταση νεότερων εκδόσεων των προβληματικών εφαρμογών. Σε αυτό το σημείο οι ειδικοί μας προτρέπουν να αναβαθμίζουμε στη νεότερη έκδοση όλες τις εφαρμογές μας, ειδικά αυτές που σχετίζονται με το Internet. Με αυτό τον τρόπο μειώνονται αρκετά οι πιθανότητες μόλυνσης.

- Δούρειοι Ίπποι

Ίσως ο μεγαλύτερος κίνδυνος μετά τους ιούς, για την πλειονότητα των χρηστών Internet, προέρχεται από τους δούρειους ίππους (Trojan horses). Πρόκειται για προγράμματα που αποτελούνται από δύο μέρη, τον πελάτη και το διακομιστή. Ο διακομιστής «φωλιάζει» με κάποιον τρόπο στον υπολογιστή του θύματος και ο πελάτης τρέχει στο μηχάνημα του θύτη. Από τη στιγμή που ο χρήστης του υπό επίθεση υπολογιστή συνδεθεί με το Internet, το Trojan-διακομιστής, που τρέχει σιωπηρά στο υπόβαθρο (background), στέλνει ένα σήμα το οποίο λαμβάνει το Trojan-πελάτης (στο μηχάνημα του θύτη). Στη συνέχεια εγκαθιδρύεται μεταξύ τους μια συνεδρία και ο κράκερ αποκτά πρόσβαση στον υπολογιστή-στόχο. Τώρα, ο μακρόθεν έλεγχος του επιτιθέμενου στο άλλο μηχάνημα ποικίλλει, αναλόγως του Trojan. Ο πρώτος μπορεί απλώς να παίζει με τα νεύρα του ανυποψίαστου χρήστη, π.χ., ανοιγοκλείνοντας το πορτάκι του οδηγού CD-ROM ή εμφανίζοντας γαργαλιστικά μηνύματα στην οθόνη του. Μπορεί όμως και να του διαγράψει αρχεία ή ακόμα και να του προκαλέσει ζημιές στο υλικό του υπολογιστή, όπως, π.χ., να του διαγράψει το BIOS ή να «χτυπήσει» τις κεφαλές του σκληρού δίσκου.

Μια άλλη, ύπουλη λειτουργία των δούρειων ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πιέζει το θύμα. Το Trojan-διακομιστής παρακολουθεί συνεχώς τις κινήσεις του χρήστη. Έτσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει για να τα στείλει αργότερα στο θύτη. Πώς όμως μπορεί να «μπει» ένα Trojan σε έναν υπολογιστή; Ο συνηθέστερος τρόπος είναι να έρχεται ως επισυναπτόμενο σε κάποιο e-mail ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, π.χ., σε ένα παιχνίδι freeware ή shareware, σε κάποιο χρήσιμο, διάσημο εργαλείο κ.λπ.

Υπάρχουν δύο τρόποι για την αποφυγή της εισβολής των Trojan. Ο πρώτος είναι η εγκατάσταση ενός πρόγραμματος «Antivirus» ή «AntiTrojan». Πολλά προγράμματα του είδους μπορούν να τα ανιχνεύουν όταν γίνεται download στον υπολογιστή ακόμα και στην περίπτωση που είναι ήδη εγκατεστημένα στο PC και να τα διαγράφουν. Ο άλλος τρόπος είναι η ύπαρξη ενός προσωπικού firewall. Κάθε φορά που ένα Trojan-διακομιστής θα προσπαθεί να «βγει» στο Internet, το firewall θα μας ειδοποιεί αναλόγως. Είναι προφανές ότι ο συνδυασμός των δύο προηγούμενων μεθόδων παρέχει τη μέγιστη προστασία. Τέλος, καλό να γίνεται εγκατάσταση στον υπολογιστή μόνο «έμπιστων» προγράμματων, από γνωστούς, επίσημους δικτυακούς τόπους.

- Μακροϊοί.

Οι Μακροϊοί γράφονται σε γλώσσα μακροεντολών ενός επεξεργαστή κειμένου, λογιστικού φύλλου ή άλλων εφαρμογών και εισέρχονται σε οποιοδήποτε τύπο εγγράφου παράγουν οι εφαρμογές. Αυτό τα μολύνει απέναντι σε οποιοδήποτε λειτουργικό σύστημα κι αν εκτελείται η εφαρμογή.

- «Κουνέλια»

Αυτά είναι προγράμματα, που όταν ξεκινήσουν, κάνουν πολλά αντίγραφα του εαυτού τους. Μπορούν να αντιγράψουν τον εαυτό τους στη μνήμη γεμίζοντας τη Ram και πιθανώς να καταρρεύσουν τον υπολογιστή. Σε αντίθεση με τους ιούς, τα κουνέλια δεν προσκολλούν τους εαυτούς τους σε υπάρχοντα αρχεία. Παρόλα αυτά, μπορεί να επιχειρήσουν να συγκαλύψουν τους εαυτούς τους υιοθετώντας ένα αθώο όνομα ή ενεργοποιώντας μια ιδιότητα της λίστας κρυφών αρχείων.

- Σκουλήκια

Είναι παρόμοια με τα κουνέλια, αλλά είναι ικανά να μεταδοθούν από ένα μηχάνημα στο άλλο επί του δικτύου εκμεταλλευόμενα λογικά κενά σε πρωτόκολλα του διαδικτύου. Τα σκουλήκια (worms) κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Συνήθως δεν μολύνουν αρχεία από τον υπολογιστή που περνούν. Πολύ γνωστές περιπτώσεις, όπως αυτές των Melissa και Love Letter, εξαπλώθηκαν στο δίκτυο με αστραπιαίο ρυθμό. Μάλιστα, το Melissa worm έχει αρχίσει ένα νέο γύρο καλυμμένο αυτήν τη φορά ως έγγραφο του Office για Mac. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε έναν υπολογιστή, στέλνουν μολυσμένα και καμουφλαρισμένα e¬mail σε όλη τη λίστα επαφών του Outlook.

Έτσι, ο ανυποψίαστος χρήστης λαμβάνει ένα e-mail από κάποιον γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο. Η μαζική αποστολή e¬mail, εκτός από την κατασπατάληση του ήδη μικρού εύρους ζώνης του modem σε ατομικό επίπεδο, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του Internet, με αποτέλεσμα να βγαίνουν συχνά εκτός λειτουργίας. Δυστυχώς, όσα μέτρα προστασίας και αν υπάρξουν, πάντοτε τα προγράμματα που χρησιμοποιούνται θα είναι ατελή, υπό την έννοια ότι θα παρουσιάζουν αδυναμίες τις οποίες ενίοτε θα εκμεταλλεύονται οι αποφασισμένοι κράκερ. Πρόκειται για τα λεγόμενα «exploits», προγραμματιστικές αδυναμίες σε γνωστές και ευρέως χρησιμοποιούμενες εφαρμογές, τα οποία μπορούν να αξιοποιούν καταλλήλως οι crackers για να αποκτούν μη εξουσιοδοτημένη πρόσβαση ή έλεγχο σε συστήματα, να προκαλούν ζημιές σε υπολογιστές-στόχους κ. ο. κ. Συχνά, πάντως, οι εταιρείες κυκλοφορούν αναβαθμίσεις ή διορθώσεις (bug fixes, patches) προγραμμάτων με γνωστά προβλήματα.

3.5 Σχεδιασμός Συστήματος Ασφαλείας για Εκτέλεση Οικονομικών Συναλλαγών

Ο σχεδιασμός του συστήματος βάσεως δεδομένων ασφαλείας για οικονομικές συναλλαγές οφείλει να αποτελεί τμήμα του αρχικού σχεδιασμού του συστήματος και όχι μια διαδικασία που θα εκτελείται μετά την εγκατάσταση του συστήματος. Οι λόγοι είναι απλοί, αφενός είναι οικονομικότερο να σχεδιάζονται και να υλοποιούνται ταυτόχρονα το σύστημα και η ασφάλεια του και αφετέρου είναι λειτουργικότερο. Ο σχεδιασμός ενός τέτοιου συστήματος στηρίζεται σε πέντε βασικά βήματα:

- Βήμα 1: Δημιουργία πολιτικής ασφαλείας
- Βήμα 2: Προσθήκη των κατάλληλων μεθόδων προστασίας ανάλογα με το πληροφοριακό σύστημα που θα χρησιμοποιήσουμε
- Βήμα 3: Σχεδίαση του συστήματος προστασίας που θα καλύπτει το φυσικό, το δικτυακό περιβάλλον και το περιβάλλον του υπολογιστικού συστήματος.

- Βήμα 4: Ανάπτυξη διαδικασιών για την παρακολούθηση, τον έλεγχο, την συντήρηση και την αναβάθμιση του συστήματος ασφαλείας.
- Βήμα 5: Χρήση των συμπερασμάτων από την παρακολούθηση και τον έλεγχο του συστήματος με στόχο την βελτίωση τόσο του σχεδιασμού, όσο και της υλοποίησης και λειτουργίας του συστήματος.

3.6 Δημιουργία Πολιτικής Ασφαλείας για Εκτέλεση Οικονομικών Συναλλαγών

Σκοπός του συστήματος ασφαλείας είναι να περιορίζει τη ροή της πληροφορίας μεταξύ δύο δικτύων. Για να δημιουργηθεί ένα firewall πρέπει εξαρχής να γίνει σαφές ποιες πληροφορίες θα μπορούν να «περάσουν» και ποιες θα μπλοκάρονται. Αυτό ονομάζεται πολιτική του φράγματος ασφαλείας. Για την πολιτική αυτή χρειάζονται στρατηγικές που μπορούν να ακολουθηθούν προκειμένου να την υλοποιηθεί:

- Εξ' ορισμού διέλευση: με τη χρήση αυτής της στρατηγικής αυτός ο οποίος χειρίζεται το firewall είναι σε θέση να μπορεί να διαχειριστεί τις πληροφορίες όπου θα εισέρχονται χρησιμοποιώντας συνθήκες προκειμένου να «μπλοκάρει» δεδομένα που δεν θέλει να εισβάλλουν στο δίκτυο του.

- Εξ΄ ορισμού απαγόρευση: σε αυτή τη στρατηγική ο διαχειριστής περιγράφει όλα τα δεδομένα, πρωτόκολλα, τα οποία επιτρέπεται να εισέλθουν στο δίκτυο του. Οτιδήποτε άλλο, δεν έχει πρόσβαση στο δίκτυο.Στη συνέχεια θα πρέπει να σχεδιαστεί το περιβάλλον που θα εγκατασταθεί η βάση δεδομένων για τις οικονομικές συναλλαγές. Με την έννοια περιβάλλον ορίζονται όσα υπάρχουν έξω από την εφαρμογή. Δηλαδή: οι υπολογιστές, τα λειτουργικά συστήματα, τα δίκτυα, καθώς και η φυσική τοποθεσία της εφαρμογής.

- Επιλογή των κατάλληλων μεθόδων προστασίας που θα χρησιμοποιηθούν. Αυτό θα υλοποιηθεί σύμφωνα με το γενικό σχεδιασμό της βάσης δεδομένων (από το δεύτερο στάδιο), την πολιτική ασφαλείας της εταιρείας γι αυτό και θα πρέπει ήδη να έχουν γίνει κατανοητές οι ανάγκες προκειμένου ο ενδιαφερόμενος να γνωρίζει τι προστασία θα χρειαστεί και ποια τεχνολογία είναι η κατάλληλη.

Για να είναι επιτυχής ο σχεδιασμός του συστήματος ασφαλείας είναι ιδιαίτερα σημαντικό να έχει ληφθεί υπόψη και να έχουν καθοριστεί οι διαδικασίες μέσα από τις οποίες θα παρακολουθείται καθημερινά η λειτουργία του και θα ελέγχεται σε τακτικά χρονικά διαστήματα η απόδοσή του. Έτσι θα γίνονται οι απαραίτητες βελτιώσεις, προσθήκες και αναβαθμίσεις.

Ανάλυση της επικινδυνότητας. Σε αυτή τη φάση θα προσδιοριστούν από την εταιρεία τα προβλήματα και οι απειλές που μπορεί να αντιμετωπίσει το σύστημα στους παρακάτω τομείς: φυσική ασφάλεια του συστήματος, ασφάλεια υπολογιστικού συστήματος, ασφάλεια βάσεων δεδομένων και τέλος ασφάλεια δικτύων επικοινωνιών.

3.7 Ανάλυση Επικινδυνότητας

Για την χάραξη της πολιτικής που ακολουθεί μια εταιρεία ή ένας οργανισμός για την υλοποίηση της ασφάλειας της βάσης δεδομένων απαιτείται η ανάλυση επικινδυνότητας, όπου θα μελετηθούν οι εκθέσεις σε κίνδυνο (exposures) του συστήματος, προσδιορίζοντας τις ευπάθειες (vulnerabilities) και τις απειλές (threats) του με βάση τον υφιστάμενο έλεγχο (control). Τα αποτελέσματα μιας ανάλυσης επικινδυνότητας (risk analysis review) της υπολογιστικής και επικοινωνιακής υποδομής της εταιρείας θα προσδιορίσουν τις απαιτήσεις ασφαλείας της βάσης δεδομένων, καλύπτοντας τις παρακάτω συνιστώσες:

- Φυσική ασφάλεια του συστήματος (physical security): Προστασία ολόκληρου του σχετικού εξοπλισμού από φυσικές καταστροφές.

- Ασφάλεια υπολογιστικού συστήματος (computer security): Προστασία των πληροφοριών της βάσης που διαχειρίζεται το λειτουργικό σύστημα (εφαρμογές, αρχεία δεδομένων, κ.ά.)

- Ασφάλεια βάσεων δεδομένων (database security): Προστασία των περιεχομένων μιας βάσης δεδομένων.

- Ασφάλεια δικτύων επικοινωνιών (network security): Προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω τοπικών, τηλεφωνικών ή άλλων δικτύων (π.χ. Internet).

3.8 Εφαρμογή Κρυπτογραφίας σε Προστασία Βάσης Δεδομένων Οικονομικών Συναλλαγών

Τα κρυπτογραφικά συστήματα για εκτέλεση οικονομικών συναλλαγών τα οποία βασίζονται στις ελλειπτικές καμπύλες για τη προστασία της βάσης δεδομένων, αποτελούν ουσιαστικά ένα πολύ σημαντικό κομμάτι της κρυπτογραφίας «δημόσιου κλειδιού» και τα τελευταία χρόνια αποκτά όλο και περισσότερο ενδιαφέρον καθώς πολλοί επιστήμονες έχουν ξεκινήσει να ασχολούνται ενεργά με τη μελέτη τους. Το πλεονέκτημα των συστημάτων αυτών σε σχέση με τα συμβατικά κρυπτογραφικά συστήματα όπως τα RSA , προσφέροντας τα ίδια επίπεδα ασφάλειας. Για το λόγο αυτό, τα κρυπτογραφικά συστήματα ελλειπτικών καμπυλών προτιμούνται τις περισσότερες φορές να χρησιμοποιούνται σε συσκευές περιορισμένων πόρων, όπως οι έξυπνες κάρτες - smart cards καθώς και στα κινητά τηλέφωνα.

Ένα από τα πιο θεμελιώδη προβλήματα στα κρυπτογραφικά συστήματα ελλειπτικών καμπυλών για τη προστασία της βάσης δεδομένων για εκτέλεση οικονομικών συναλλαγών, είναι ουσιαστικά η γένεση ελλειπτικών καμπυλών, κατάλληλων να προσφέρουν την ασφάλεια που απαιτείται από τις κρυπτογραφικές εφαρμογές. Η πιο αποδοτική μέθοδος της γένεσης ελλειπτικών καμπυλών, ορισμένων πάνω σε πρώτα, πεπερασμένα σώματα, είναι η μέθοδος του Μιγαδικού Πολλαπλασιασμού ή εν συντομία η μέθοδος CM. Η μέθοδος αυτή απαιτεί ουσιαστικά την εύρεση των ριζών ορισμένων πολυωνύμων, που ονομάζονται πολυώνυμα κλάσεως.

Θα πρέπει στο σημείο αυτό να αναφερθεί πως η μέθοδος της «Κρυπτογράφησης» χρησιμοποιείται από τους ειδικούς των επιχειρήσεων με σκοπό την προστασία των πηγών τους και των αρχείων που βρίσκονται στους ηλεκτρονικούς τους υπολογιστές. Τα αρχεία αυτά έχουν προηγουμένως αποθηκευτεί και βρίσκονται εντός των αρχείων προγραμμάτων και επικοινωνιών και μπορούν να περιλαμβάνουν κάποιο σημαντικό ηλεκτρονικό ταχυδρομείο, παγκόσμιες τραπεζικές συναλλαγές, δίκτυα εταιρειών καθώς και απόρρητες τηλεφωνικές κλήσεις. Κάποια από τα συστήματα κρυπτογράφησης που βρίσκονται σε παγκόσμια βάση, έχουν την ικανότητα να κρυπτογραφούν κάθε λεπτομέρεια στον σκληρό τους δίσκο και να προστατεύουν τον υπολογιστή σε μεγάλο βαθμό. Μέσω αυτής της μεθόδου, ο υπολογιστής τίθεται σε αχρηστία και κανένας από τους μη εξουσιοδοτημένους χρήστες δεν έχει την ικανότητα να παρέμβει και να επεξεργαστεί ή να υποκλέψει οποιαδήποτε στοιχεία. Ακόμη και στην περίπτωση που ένας υπολογιστής κλαπεί, τα αρχεία που αυτός διαθέτει στην μνήμη του δεν διατρέχουν άμεσο κίνδυνο.

Η μέθοδος της κρυπτογράφησης για τη προστασία της βάσης δεδομένων για εκτέλεση οικονομικών συναλλαγών θεωρείται τόσο σημαντική και δυνατή, όσο και εκείνη της εφαρμογής ενός λογισμικού και ενός σκληρού δίσκου. Η συγκεκριμένη μέθοδος μπορεί να εμφανίζεται τόσο ως εφαρμογή κρυπτογράφησης αλλά και πακέτο λογισμικού. Βέβαια η μέθοδος αυτή δεν δρα πάντα από μόνη της, αφού διάφορα άλλα πακέτα λογισμικού και προϊόντα ηλεκτρονικών υπολογιστών μπορούν να βοηθήσουν στην λειτουργία της.

Η κρυπτογραφία για τη προστασία της βάσης δεδομένων αναφέρεται στην υλοποίηση μεθόδων τροποποίησης των μεταδιδομένων πληροφοριών, έτσι ώστε να γίνονται κατανοητά μόνο από τον προβλεπόμενο παραλήπτη ή παραλήπτες. Είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο σε hardware όσο και σε software. Η ενσωμάτωση των μεθόδων της κρυπτογραφίας σε hardware επιταχύνει σε μεγάλο βαθμό την διεκπεραίωση της. Επίσης, οι χρήστες δεν γνωρίζουν, ούτε καν αντιλαμβάνονται την παρουσία της και πραγματοποιούν ανενόχλητοι τις εργασίες τους σκληρό δίσκο, για ασφαλής συναλλαγές μέσω του διαδικτύου ή ακόμα και για τη σύνδεση με καλωδιακή τηλεόραση.

Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας για εκτέλεση οικονομικών συναλλαγών είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη την διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει γνώση αυτού. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία. Οι τρόποι άμυνας και πρόληψης που χρησιμοποιούνται συνήθως από τις επιχειρήσεις για τις παραπάνω κατηγορίες με τη συμβολή της κρυπτογραφίας για τη προστασία της βάσης δεδομένων και ενάντια του «πληροφοριακού πολέμου» για εκτέλεση οικονομικών συναλλαγών, αναφέρονται στις παρακάτω εξής περιπτώσεις:

- Πρόληψη
- Αποτροπή
- Ενδείξεις και προμηνύματα
- Ανακάλυψη
- Προετοιμασία για επείγοντα περιστατικά
- Απάντηση

Οι συγκεκριμένες κατηγορίες είναι αλληλένδετες μεταξύ τους και ορισμένοι από τους μηχανισμούς χρησιμοποιούνται σε περισσότερες από μια κατηγορίες. Εξαίρεση αποτελεί η περίπτωση όπου εντοπίζονται τα περισσότερα έξοδα και τα οποία

επιβάλλονται για την λήψη των κατάλληλων και απαιτούμενων μέτρων. Φυσικά δύναται να υπάρξουν περισσότερα έξοδα και τα οποία είναι λίγο δύσκολο να προσδιοριστούν αναλόγως.

Ο πρώτος τρόπος αντιμετώπισης των μεθόδων «πληροφοριακού πολέμου» για τη προστασία της βάσης δεδομένων, είναι εκείνος της Πρόληψης. Ο συγκεκριμένος τρόπος αποβλέπει στην αποφυγή μιας εκδήλωσης επίθεσης η οποία αιωρείται ουσιαστικά στον επιτιθέμενο μια πρόσβαση στην πηγή των πληροφοριών. Ο μηχανισμός που εμπλέκεται σε αυτόν τον τρόπο άμυνας, περιλαμβάνει την απόκρυψη σημαντικών πληροφοριών, τον έλεγχο εισόδου από τους χρήστες αλλά και την πιστοποίηση τους.

Ο δεύτερος τρόπος αντιμετώπισης, είναι εκείνος που αναφέρεται στην Αποτροπή. Η συγκεκριμένη μέθοδος στοχεύει στην τοποθέτηση αντιμετώπισης μιας μη ελκυστικής επίθεσης για ανάκτηση πηγών πληροφοριών. Στην κατηγορία αυτή εσωκλείονται οι νόμοι, οι ποινές που επέρχονται από αυτούς αλλά και οι αποζημιώσεις που μπορούν να προκύψουν. Ο έλεγχος ασφαλείας που μπορεί να λάβει χώρα σε αυτή την περίπτωση, διεξάγεται προληπτικά αφού ένας πιθανός επιτιθέμενος μπορεί να διαπιστώσει πως ενδεχομένως δεν χρειάζεται να εισχωρήσει σε κάποιο σύστημα και να κινδυνέψει για αυτό, αφού οι πληροφορίες που θα ανακτήσει ίσως να μην είναι αρκετά σημαντικές.

Ο τρίτος τρόπος αντιμετώπισης τέτοιων φαινομένων για τη προστασία της βάσης δεδομένων, είναι οι Ενδείξεις και τα Προμηνύματα. Ο τρόπος αυτός λειτουργεί ως εργαλείο αναγνώρισης μιας επίθεσης από έναν απρόσμενο και ανεπιθύμητο παράγοντα. Μέσω αυτού του εργαλείου, μπορούν να παρθούν συγκεκριμένα μέτρα και νόμοι προκειμένου να αποτραπεί ή να καταστεί αδύνατη η επίθεση από αυτούς τους ανεπιθύμητους παράγοντες. Συνήθως οι κυβερνήσεις είναι αυτές που εφαρμόζουν τα μέτρα αυτά και ζητούν πληροφορίες από επιχειρήσεις και οργανισμούς που παρακολουθούν τέτοιου είδους επιθέσεις.

Ο τέταρτος τρόπος αντιμετώπισης, είναι εκείνος της Ανακάλυψης. Οι εισπράξεις χρηματικών ποσών της επιχείρησης από τις δημόσιες υπηρεσίες σε πολλές περιπτώσεις ταυτίζονται με αυτές των πολιτών, κατ' αναλογία των πληρωμών, τόσο ως προς τα αντικείμενα των πληρωμών όσο και ως τους τρόπους πληρωμής. Στην περίπτωση των επιχειρήσεων που δεν είναι ατομικές, η επιχείρηση πρέπει να εκπροσωπείται από τον νόμιμο εκπρόσωπο της. Έτσι ενώ στην πράξη κάτι τέτοιο χρειάζεται μια πληθώρα διοικητικών εγγράφων και φυσική παρουσία στη ΔΟΥ, στις ηλεκτρονικές υπηρεσίες απαιτεί εξειδικευμένες τεχνολογίες ταυτοποίησης και αυθεντικοποίηση των χρηστών μέσω της κρυπτογράφησης.

Η ανακάλυψη έχει και εκείνη σχεδόν τον ίδιο σκοπό με τις Ενδείξεις και τα Προμηνύματα και την στενή παρακολούθηση μιας επίθεσης μετά την έναρξη της. Τα εργαλεία που χρησιμοποιούνται σε αυτό τον τρόπο αντιμετώπισης, έχουν την ικανότητα να λειτουργούν μεθόδους, οι οποίες μπορούν να εντοπίζουν επιβλαβείς ή ψευδείς πληροφορίες και εν συνεχεία να επεξεργάζονται τις εισερχόμενες πληροφορίες.

Η πέμπτη κατηγορία αντιμετώπισης των μεθόδων «πληροφοριακού πολέμου» για τη προστασία της βάσης δεδομένων, είναι αυτή της Προετοιμασίας για επείγοντα περιστατικά. Ο τρόπος αυτός σχετίζεται άμεσα με την δυνατότητα ενός συστήματος για ανάκαμψη μετά την επίθεση που θα δεχθεί αλλά και την απάντηση του σε αυτό. Στην κατηγορία αυτή συγκαταλέγονται και η λήψη των αντιγράφων αλλά και η διόρθωση μιας βλάβης μετά από μια ισχυρή επίθεση. Με αυτόν τον τρόπο όμως δεν θεωρείται πιθανή η πρόβλεψη ή η πρόληψη κάθε επίθεσης. Ο αμυντικός

«πληροφοριακός πόλεμος» σχετίζεται άμεσα με την σωστή διαχείριση των κινδύνων αλλά όχι με την αποφυγή τους, σε οποιοδήποτε κόστος κάτι τέτοιο θα είναι αποδεκτό.

3.9 Μηχανισμός Steam Ciphers για τη Προστασία της Βάσης Δεδομένων για Εκτέλεση Οικονομικών Συναλλαγών

Για την προστασία βάσης δεδομένων μπορεί να χρησιμοποιηθεί ένας τύπος αλγορίθμου όπως ο Stream Cipher. Είναι αρκετά γρήγορος αλγόριθμος και ξεπερνάει κατά πολύ και τους block ciphers. Μια ειδοποιός διαφορά είναι ότι οι block ciphers λειτουργούν με μεγάλα κομμάτια δεδομένων (blocks) ενώ οι stream ciphers λειτουργούν με μικρότερα κομμάτια απλού κειμένου δηλαδή με bits. Η κρυπτογράφηση με έναν stream cipher υλοποιείται με τον μετασχηματισμό των μικρότερων αυτών μονάδων οι οποίοι ποικίλουν ανάλογα με το πότε αντιμετωπίζονται κατά την διάρκεια της κρυπτογράφησης. Σε αντίθεση με έναν block η κρυπτογράφηση ενός συγκεκριμένου κειμένου θα καταλήγει πάντα στο ίδιο αποτέλεσμα όταν χρησιμοποιείται το ίδιο κλειδί. Ο πιο ευρέως χρησιμοποιούμενος stream cipher είναι ο RC4.

3.10 Άλλοι Τρόποι προστασίας Πληροφοριακών Συστημάτων

Τέλος αξίζει να αναφερθούν και κάποιοι άλλοι τρόποι προστασίας των Πλήροφοριακών Συστημάτων κατά την περίπτωση των Οικονομικών Συναλλαγών:

- Φίλτρα πρόσβασης στα συστήματα της Τράπεζας - Firewalls

Είναι εξοπλισμός hardware & software που παρεμβάλλεται μεταξύ του Internet και των συστημάτων της Τράπεζας και φιλτράρουν τα δεδομένα που κυκλοφορούν σύμφωνα με τις πολιτικές ασφαλείας που καθορίζει η Τράπεζα και τα διεθνή πρότυπα. Με αυτό το φιλτράρισμα προστατεύονται όλα τα σημεία του δικτύου της Τράπεζας στα οποία ο εξωτερικός και εσωτερικός μη εξουσιοδοτημένος χρήστης δεν πρέπει να έχει πρόσβαση.Η υπηρεσία eBanking προστατεύεται από Firewalls τελευταίας τεχνολογίας, που αποτελούν σήμερα τα καλύτερα φίλτρα ελέγχου πρόσβασης στο σύστημα της Τράπεζας.

- Εικονικό πληκτρολόγιο

Το εικονικό πληκτρολόγιο είναι ένα κανονικό πληκτρολόγιο που εμφανίζεται στην οθόνη του υπολογιστή και δίνει τη δυνατότητα να το χρησιμοποιηθεί για τη συμπλήρωση συγκεκριμένα στοιχεία στην οθόνη εισόδου στην υπηρεσία eBanking, αντικαθιστώντας το πραγματικό πληκτρολόγιο που είναι συνδεδεμένο με τον υπολογιστή σας. Το εικονικό πληκτρολόγιο εμφανίζεται στην οθόνη εισόδου της υπηρεσίας eBanking για να συμπληρώσετε μέσω αυτού τους κωδικούς πρόσβασής σας στην υπηρεσία. Με τον τρόπο αυτό αποτρέπεται κάθε δυνατότητα υποκλοπής των κωδικών σας, μέσω ιών που μπορούν να καταγράψουν τις πληκτρολογήσεις από το πραγματικό πληκτρολόγιο.

- Αυτόματος Τερματισμός Επικοινωνίας με την υπηρεσία eBanking

Όταν δεν χρησιμοποιείται ένα σύστημα με το οποίο είστε συνδεδεμένος για συγκεκριμένο χρονικό διάστημα, διακόπτεται αυτόματα η σύνδεσή σας για λόγους ασφαλείας.Η επικοινωνία σας με την υπηρεσία eBanking τερματίζεται αυτόματα εφόσον δεν πραγματοποιήσετε κάποια ενέργεια μέσω αυτής για διάστημα 15 λεπτών. Ο υπολειπόμενος χρόνος παραμονής σας στο σύστημα εμφανίζεται στη μπάρα χρόνου, απ' όπου μπορεί να ανανεωθεί.

- Κλείδωμα κωδικών πρόσβασης

Όταν καταχωρούνται λανθασμένα συνεχόμενες φορές οι κωδικοί πρόσβασης σε ένα σύστημα κλειδώνονται, ώστε αν κάποιος προσπαθεί να μαντέψει τους κωδικούς αυτούς να μην έχει απεριόριστες προσπάθειες. Οι κωδικοί πρόσβασης στην υπηρεσία eBanking (user name και PIN) κλειδώνονται αυτόματα στις 3 συνεχόμενες λανθασμένες καταχωρήσεις τους στην οθόνη εισόδου της υπηρεσίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΞΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Adams, J., 1998, "*The next world war*", Simon and Schuster
2. BloomBecker, B., 1990, "*Spectacular Computer Crimes*", Dow Jones – Irwin
3. Cavoukian, A., Tapscott, D., 1997, "*Who Knows",* McGraw-Hill
4. Denning, D., E., 2007, "*Cryptography and Data Security*", Addison – Wesley
5. Diffie, W., Landau, S., 1998, "*Beyond Calculation*", The MIT Press
6. Hager, N., 1996, "*Secret Power*", Craig Cotton Publishing, New Zealand, 1996
7. Kesler, R., 1988, "*Spy vs. Spy*", Pocket Books
8. Libicki, G., M., 1995, "*What information is warfare?",* National Defense University of USA
9. Ludlow, P., 1996, "*High Noon on the Electric Frontier*", The MIT Press
10. McCarthy, L., 1997, "*Intranet Security*", Prentice Hall
11. Meinel, C., P., 1998, "*The Happy Hacker",* American Eagle Publications
12. Mihir Bellare, Gregory Neven: Transitive signatures: new schemes and proofs. IEEE Transactions on Information Theory 51(6): 2133-2151 (2005)
13. Pfleeger, C., P., 1997, "*Security in Computing*", Prentice Hall
14. Ransom, A. W., 1994, "*Who Owns Information*", Basic Books
15. Rosenoer,J., 1997 "*Cyber Law*", Springer – Verlag
16. Schneier, B., 1996, "*Applied Cryptography*", Prentice Hall
17. Schweizer, P., 1993, "*Friendly Spies*", The Atlantic Monthly Press
18. Slade, P., 1994, "*Guide to Computer Viruses*", Springer – Verlag
19. Sterling, B., 1992, "*The Hacker Crackdown*", Bantam
20. Taylor,A., 1999, "*The Hackers*", Routledge
21. Timpton, H., F., Ruthberg, Z., G., 1993, "*Handbook of Information Security Management*", Acerbic

ΕΛΛΗΝΙΚΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

22. Α. Πασχόπουλος και Π. Σκαλτσάς 2006, "*Ηλεκτρονικό Εμπόριο*", εκδόσεις Κλειδάριθμος.
23. Α. Πομπόρτσης 2005, "*Εισαγωγή στην Ηλεκτρονική Διακυβέρνηση*", εκδόσεις Τζιόλα.
24. Α. Πομπόρτσης, Α. Τσούλφας 2002, "*Εισαγωγή στο Ηλεκτρονικό Εμπόριο*",Τζιόλα.
25. Μ. Βλαχοπούλου 2008, "*Ε-Μάρκετινγκ, Διαδικτυακό Μάρκετινγκ*", εκδόσεις Rosili.
26. Μπερμπερίδης Τιμόθεος 2007 "*ΧΡΗΜΑ*", Μηνιαίο Οικονομικό και Επενδυτικό Περιοδικό, "*Η Λήψη Χρηματοικονομικών Αποφάσεων και Χρηματοοικονομική Ισορροπία*", Αθήνα, Νοέμβριος
27. Singh Simon, "Κώδικες και μυστικά", Τραυλός

INTEPNET

28. http://el.wikipedia.org
29. http://www.digisigner.com/
30.http://www.digitalgreece2020.gr
31. www.verisign.com