ΠΕΡΙΛΗΨΗ

Αντικείμενο της εργασίας αυτής είναι η ασφάλεια στο ηλεκτρονικό εμπόριο. Εξετάζονται οι *κίνδυνοι* που πηγάζουν από την αθρόα και απρόσωπη διεξαγωγή συναλλαγών που αφορούν το ηλεκτρονικό εμπόριο. Στη συνέχεια γίνεται αναφορά στους τρόπους με τους οποίους κάποιος μπορεί να προφυλαχθεί από αυτές τις απειλές που καραδοκούν στο διαδίκτυο. Τέτοιοι τρόποι είναι *η κρυπτογράφηση*, *οι ψηφιακές υπογραφές*, *τα ψηφιακά πιστοποιητικά* αλλά και η *χρησιμοποίηση κλειδιών* όπως το PKI και το IPSec και *πρωτοκόλλων* όπως το SSL και το SET. Τα τελευταία μάλιστα αποδεικνύονται ιδιαίτερα χρήσιμα στις ηλεκτρονικές πληρωμές. Στη συνέχεια διεξάγεται μία σύγκριση μεταξύ των πιο δημοφιλών *Firewalls* καθώς και επιχειρείται προσπάθεια ερμηνείας της λειτουργίας τους. Αναφορά επίσης γίνεται και στα συστήματα *RADIUS και TACACS+* καθώς και στις διαφορές τους. Το επόμενο θέμα αφορά την προστασία που είναι δυνατόν να παρασχεθεί σε ένα χρήστη όσον αφορά την *ηλεκτρονική του αλληλογραφία* και τους *ιούς* που κινούνται ανεξέλεγκτα στο διαδίκτυο. Τέλος, ένα αντικείμενο μελέτης της εργασίας αυτής είναι η σχέση του ηλεκτρονικού εμπορίου με *τα προσωπικά δεδομένα* κάθε χρήστη καθώς και ποια θα πρέπει να είναι *η πολιτική ασφάλειας* για την καλύτερη αντιμετώπιση των κινδύνων που πηγάζουν από το ηλεκτρονικό εμπόριο.

SUMMARY

The main object of this research is the security in e-commerce. Firstly it surveys the *threats* that come of the continuous and impersonal conduct of transactions that concern e-commerce. Next, there are some references on how someone could protect himself and of course his computer from these threats that take place in the Internet. Such ways are the *encryption*, *the digital signatures*, *the digital certificates* and also the use of keys such as *PKI* and *IPSec* and *protocols* such as *SSL* and *SET*. The last two indeed prove very useful in electronic payments. Next, there is a comparison between the most popular *Firewalls* and also it is tried an explanation of its action. Reference also is made on the systems *RADIUS* and *TACACS+* and also about their differences. The next subject is about the protection that is possible to be provided to a server in regard to his *e-mail* and the *viruses* that move uncontrollably on Web. Lastly, an object of research is the relation between e-commerce and *personal data* and also what should be the *security policy* of every user in terms of a better co frontal with the threats that come of e-commerce.

1. Εισαγωγή

ΤΟ ΔΙΑΔΙΚΤΥΟ , ΟΧΙ ΠΟΛΛΑ ΧΡΟΝΙΑ ΠΡΙΝ, ΑΠΟΤΕΛΟΥΣΕ ένα κατά πολύ μικρότερο «μέρος» συγκριτικά με σήμερα. Οι κόμβοι του ήταν διεσπαρμένοι σε ακαδημαϊκά ιδρύματα, ερευνητικά εργαστήρια και εταιρείες που περιλάμβαναν φοιτητές, ερευνητές και γενικότερα ανθρώπους που ασχολούνταν κατά τον έναν ή τον άλλο τρόπο με την τεχνολογία και τις επιστήμες. Η υποδομή του, το διάσημο ζεύγος πρωτοκόλλων TCP/IP, είχε σχεδιαστεί για να λειτουργεί απλά και αποτελεσματικά.

Σύντομα, το Διαδίκτυο ξέφυγε από τα στενά ακαδημαϊκά και ερευνητικά πλαίσια, κερδίζοντας τις καρδιές ολοένα και περισσότερων απλών χρηστών ακόμα και ανθρώπων που δεν είχαν άμεση σχέση με την τεχνολογία και τους υπολογιστές. Η πολυπλοκότητα του ως συστήματος, με την ευρύτερη έννοια, άρχισε να αυξάνει με γοργό ρυθμό, κάνοντας φανερό ότι θα εξαπλωθεί, θα παρεισφρήσει και θα αγκαλιάσει κάθε πλευρά της κοινωνικής και οικονομικής ζωής. Έτσι και έγινε. Όπως όμως συμβαίνει και με άλλα συστήματα στη φύση αλλά και στις ανθρώπινες κοινωνίες, από την αύξηση της πολυπλοκότητας δεν προέκυψαν μόνον επιθυμητές «ιδιότητες». Όταν το σύστημα διαβεί ένα συγκεκριμένο κατώφλι -το οποίο, μάλιστα, δύσκολα μπορεί να γίνει διακριτό έκτων προτέρων-, οι προκύπτουσες ιδιότητες γίνονται δυνητικά επιβλαβείς για τους συμμετέχοντες (και μη) στο σύστημα, ακόμα και για την ίδια την υπόσταση του. Εν προκειμένω, κανείς δεν αμφιβάλλει ότι το Διαδίκτυο αποτελεί ένα πολύπλοκο σύστημα. Εκτείνεται σε ολόκληρο τον πλανήτη, μεταβάλλοντας τη σημασία του χώρου και του χρόνου, φέρνοντας κοντά εκατομμύρια ανθρώπους με διαφορετικό πολιτισμικό, οικονομικό και κοινωνικοπολιτικό υπόβαθρο. Όλοι αυτοί επικοινωνούν, διασκεδάζουν, εκπαιδεύονται, πληροφορούνται και διεξάγουν τις όποιες οικονομικές ή επιχειρηματικές δραστηριότητες τους στο οικουμενικό αυτό μέσο.[2]

ΚΙΝΔΥΝΟΙ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

Σε ένα συνεχώς διευρυνόμενο μέσο όπως το Διαδίκτυο με τα κεφάλαια για επενδύσεις στην ιδέα του ηλεκτρονικού επιχειρείν να ρέουν άφθονα και συνεχώς, υπάρχει μεγάλο περιθώριο για κέρδος αλλά και για… χάσιμο. Μέσα σ' αυτό το κλίμα, όπου αυξάνονται και οι ευκαιρίες για (ηλεκτρονική) απάτη, οι επιτήδειοι δεν λείπουν ποτέ.

Οι επιθέσεις περιληπτικά

Κατηγορία	Πηγή	Στόχος	Επικινδυνότητα	Κίνδυνοι	Αντιμετώπιση
Επιθέσεις σε διακομιστές και εταιρικά δίκτυα	Κράκερ από το Internet	Διακομιστές	Υψηλή	Απώλεια δεδομένων, διακοπή υπηρεσιών	Εγκατάσταση firewall, χρήση κωδικών πρόσβασης, επιτήρηση λογισμικού
Μη εξουσιοδοτημένη πρόσβαση	Τοπικό δίκτυο, Internet	Όλοι οι χρήστες	Υψηλή	Κατάληψη μηχανημάτων, παραβίαση του απορρήτου, μηχανήματα εκτίθενται στο τοπικό δίκτυο	Εγκατάσταση firewall, φειδωλή χρήση των κοινόχρηστων φακέλων και εκτυπωτών, χρήση «καλών» κωδικών
Ιοί, σκουλήκια (worms) και δούρειοι ίπποι (Trojan horses)	Ηλεκτρονική αλληλογραφία, λογισμικό που κατεβάζουμε από το Internet	Όλοι οι χρήστες	Μέτρια έως και υψηλή	Παρακολούθηση ενεργειών, απώλεια δεδομένων	Χρήση «αντιβιοτικών» και firewall
Παρακολούθηση e-mail	Κράκερ από το Internet ή το τοπικό δίκτυο	Όλοι οι χρήστες	Μέτρια έως και υψηλή	Μη εξουσιοδοτημένοι χρήστες μπορούν να διαβάζουν το e-mail από ενδιάμεσους διακομιστές	Κρυπτογράφηση μηνυμάτων, χρήση «καλών» κωδικών, περιορισμός της φυσικής πρόσβασης σε μηχανήματα
Παρακολούθηση πληκτρολόγησης	Δούρειοι ίπποι, χρήστες που έχουν φυσική πρόσβαση στο μηχάνημα	Όλοι οι χρήστες	Υψηλή	Παρακολουθείται οτιδήποτε πληκτρολογείται, έτσι γίνονται γνωστοί διάφοροι κωδικοί πρόσβασης	Χρήση προγραμμάτων για τον εντοπισμό δούρειων ίππων, έλεγχος της φυσικής πρόσβασης

Πίνακας 1.1: Κίνδυνοι στο ηλεκτρονικό εμπόριο[2]

Χαρακτηριστικά παραδείγματα επιθέσεων σε διαδικτυακά συστήματα (και μάλιστα πολύ γνωστών οργανισμών και εταιρειών) είναι τα παρακάτω:

i. Μια κοινή έρευνα από το FBI και το ίδρυμα ασφάλειας υπολογιστών τύχης (CSI) σε 500 επιχειρήσεις ανέφερε ότι 42 τοις εκατό των εναγομένων είχαν εκθέσει την αναρμόδια χρήση των συστημάτων πληροφοριών τους. Ακόμα πιο καταπληκτικά, 32 τοις εκατό των εναγομένων δήλωσαν ότι έχασαν πάνω από $100 εκατομμύρια λόγω των ηλεκτρονικών παραβιάσεων ασφάλειας.

ii. Τον Αύγουστο του 1996, το τμήμα ιστοχώρου της δικαιοσύνης (DOJ) (http://www.usdoj.gov/) παραβιάστηκε από χάκερ που εισχώρησαν στη μηχανή οικοδεσποτών Ιστού του DOJ [Edupage συντάκτες 1996]. Οι χάκερ εκμεταλλεύθηκαν την ευκαιρία και τοποθέτησαν αγκυλωτούς σταυρούς, άσεμνες εικόνες, και την κριτική του νόμου ευπρέπειας επικοινωνιών. Η διείσδυση οδήγησε στο προσωρινό κλείσιμο της περιοχής έως ότου μπόρεσε να αξιολογηθεί η ζημία και ο ιστοχώρος να αποκατασταθεί. Έναν μήνα αργότερα, ο ιστοχώρος CIA (http://www.odci.gov/ cia) παραβιάστηκε από μια ομάδα σουηδών χάκερ που διαμαρτύρονταν για μια σουηδική δικαστική υπόθεση ενάντια σε μια ομάδα νεολαιών που συλλήφθηκε για τα εγκλήματα ασφάλειας υπολογιστών το 1991 [Neumann 1996]. Η σελίδα έγραφε "σελίδα υποδοχής Ιστού στην κεντρική αντιπροσωπεία ηλιθιότητας". Υπήρχαν επίσης συνδέσεις με τον ιστοχώρο Playboy, τους ιστοχώρους διαφόρων χάκερ αλλά και σπασμένες συνδέσεις τοποθετήθηκαν επίσης στη σελίδα. Συμπτωματικά, την ημέρα που ο ιστοχώρος CIA παραβιάστηκε ήταν η ημέρα που το DOJ ξανάβαλε τον ιστοχώρο του στο δίκτυο.

iii. Τον Δεκέμβριο του 1996 βεβαιώθηκε η πτώση ενός άλλου κυβερνητικού ιστοχώρου. Ο ιστοχώρος της Πολεμικής Αεροπορίας των Η.Π.Α. (http://www.af.mil/) [Neumann 1997]. Η αλλαγμένη κεφαλίδα της ιστοσελίδας ήταν, "καλωσορίσατε στην αλήθεια" επάνω από τη γραφική παράσταση που έδειχνε αίματα και ένα ζευγάρι βολβών ματιού. Ένα κείμενο που προστίθεται στη σελίδα ήταν, "μπορείτε να μάθετε τα πάντα για την κυβερνητική δωροδοκία εδώ. Μάθετε τα μυστικά που δεν θέλουν να ξέρετε". Η γραφική παράσταση περιέλαβε μια X-rated εικόνα με τον τίτλο, "αυτό είναι αυτό που η κυβέρνησή κάνει σε σας κάθε ημέρα.[1]

Προκειμένου λοιπόν να αποφευχθούν καταστάσεις σαν τις παραπάνω καλό είναι να ληφθούν κάποια μέτρα ασφαλείας. Αυτά τα μέτρα θα πρέπει να έχουν τους παρακάτω στόχους.

ΣΤΟΧΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ

- *Εμπιστευτικότητα (confidentiality):* Διασφάλιση της προσπελασιμότητας της πληροφορίας μόνο από όσους έχουν τα απαραίτητα δικαιώματα.
- *Ακεραιότητα (integrity):* Διαφύλαξη της ακρίβειας και της πληρότητας της πληροφορίας και των μεθόδων επεξεργασίας αυτής.
- *Διαθεσιμότητα (availability):* Διασφάλιση της προσπελασιμότητας της πληροφορίας σε εξουσιοδοτημένους χρήστες όποτε απαιτείται.
- *Έλεγχος αυθεντικότητας (authentication):* Εξακρίβωση της ταυτότητας του χρήστη είτε με passwords είτε με προσωπικούς αριθμούς αναγνώρισης (Personal Identification Numbers - PIN's) και διάφορα άλλα.
- *Μη αποποίηση της ευθύνης (non – repudiation):* Ολοκλήρωση συναλλαγής όπου κάποιος μετά δεν μπορεί να ισχυρισθεί ότι δεν συμμετείχε σ' αυτήν.
- *Εξουσιοδότηση (authorization):* Παραχώρηση δικαιωμάτων στο χρήστη από τον ιδιοκτήτη.[9]

2. ΣΥΣΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Με βάση λοιπόν τους παραπάνω στόχους θα πρέπει να ενεργεί κάποιος που ενδιαφέρεται να διασφαλίσει τις συναλλαγές του στο δίκτυο και να αποφύγει τους κινδύνους που αναφέρθηκαν παραπάνω. Προκειμένου λοιπόν να εξουδετερωθούν αυτές οι απειλές έχει αναπτυχθεί ένας ικανός αριθμός πρωτοκόλλων και εφαρμογών βασισμένων κυρίως σε τεχνικές κρυπτογράφησης.

Πρότυπα ασφάλειας για το Διαδίκτυο

Πρότυπο	*Λειτουργία*	*Εφαρμογή*
Secure HTTP (S-http)	Καθιστά ασφαλείς τις web συναλλαγές	Browsers, web servers και Internet εφαρμογές
Secure Sockets Layer (SSL)	Παρέχει ασφάλεια σε πακέτα δεδομένων στο επίπεδο δικτύου	Browsers, web servers και Internet εφαρμογές
Secure MIME (S/MIME)	Καθιστά τα προσαρτημένα σε μηνύματα ηλεκτρονικού ταχυδρομείου αρχεία ασφαλή (secure mail attachments)	Πακέτα ηλεκτρονικού ταχυδρομείου με RSA κρυπτογράφηση και ψηφιακές υπογραφές
Secure Electronic Transactions (SET)	Εγγυάται ασφάλεια σε συναλλαγές με πιστωτικές κάρτες	Έξυπνες κάρτες, Transaction Servers

Πίνακας 2.1: Πρότυπα Ασφαλείας[7]

3. ΑΣΦΑΛΕΙΑ ΣΤΟ WEB

ΠΡΩΤΟΚΟΛΛΟ ΜΕΤΑΦΟΡΑΣ HYPER TEXT(S-HTTP)

Το ασφαλές πρωτόκολλο μεταφοράς Hyper Text (S-HTTP) είναι μια ασφαλής επέκταση του HTTP που εξυπηρετεί ιστοσελίδες. Το S-HTTP αναπτύχθηκε από την Enterprise Integration Technologies, εμπορευματοποιήθηκε από Terisa Systems (http://www.terisa.com/) και διανεμήθηκε στην κοινοπραξία δικτύου εμπορίου. Από μόνο του, το HTTP δεν παρέχει ασφαλείς ιδιότητες για τις συναλλαγές στο Web . Οι κεντρικοί υπολογιστές δικτύου μπορούν να εφαρμόσουν μερικές ασφαλείς ιδιότητες όπως ο βασικός έλεγχος πρόσβασης. Οι μηχανισμοί ελέγχου πρόσβασης μπορούν να αποτρέψουν την αναρμόδια πρόσβαση σε έναν κεντρικό υπολογιστή, αλλά δεν παρέχουν την εμπιστευτικότητα στις συναλλαγές στοιχείων. Χωρίς μερικά μέσα για τη συναλλαγή στοιχείων, οι κωδικοί πρόσβασης που χρησιμοποιούνται στις ασφαλείς μερίδες πρόσβασης ενός κεντρικού υπολογιστή μπορούν να συλληφθούν στο σαφές κείμενο από τους τρίτους και να χρησιμοποιηθούν στη συνέχεια για να αρπάξουν τα εμπιστευτικά στοιχεία. Το S-HTTP παρέχει ασφαλή μέσα για τους πελάτες ώστε να επικοινωνήσουν με τους κεντρικούς υπολογιστές δικτύου. Αντίθετα από τη SSL, το S-HTTP τρέχει στο στρώμα εφαρμογής παράλληλα με το HTTP και άλλες υπηρεσίες δικτύων. Το σχήμα 3.1 παρουσιάζει τη σχέση του S-HTTP, του HTTP, άλλων υπηρεσιών δικτύων, του SSL και των ασφαλών συστημάτων πληρωμής.

Το S-HTTP παρέχει μέσα για ασφαλή επικοινωνία με έναν κεντρικό υπολογιστή δικτύου. Το πρωτόκολλο σχεδιάστηκε για να είναι αρκετά γενικό ώστε να παρέχει ευρεία υποστήριξη για διάφορες ασφαλείς τεχνολογίες, συμπεριλαμβανομένης της συμμετρικής κρυπτογράφησης για την εμπιστευτικότητα στοιχείων, τη δημόσια βασική κρυπτογράφηση για την επικύρωση πελατών/ κεντρικών υπολογιστών, και τις αφομοιώσεις μηνυμάτων για την ακεραιότητα στοιχείων. Αυτές οι τεχνολογίες μπορούν να χρησιμοποιηθούν μεμονωμένα ή σε συνδυασμό κατά τη διάρκεια μιας συναλλαγής. Το S-HTTP είχε ως σκοπό επίσης να είναι διαλειτουργικό με τις

υπηρεσίες HTTP που ήταν μη-ασφαλείς. Αυτό σημαίνει ότι το S-HTTP μπορεί να χρησιμοποιηθεί ως μέσο πρόσβασης ιστοσελίδας ακόμα και σ' αυτές που δεν εφαρμόζουν το πρωτόκολλο S-HTTP για τις μη-ασφαλείς επικοινωνίες. Κάποιο συμβαλλόμενο μέρος μπορεί επίσης να διευκρινίσει τις ασφαλείς τεχνολογίες. Με άλλα λόγια, ένας πελάτης μπορεί να διευκρινίσει ότι η σύνοδος ιστού(web session) απαιτεί την εμπιστευτικότητα μέσω της συμμετρικής βασικής κρυπτογράφησης, ενώ ο κεντρικός υπολογιστής μπορεί να απαιτήσει την επικύρωση πελατών μέσω του δημόσιου βασικού συστήματος κρυπτογραφίας.

	Πρωτόκολλα πληρωμής (SET, CyberCash, FirstVirtual,…)		
S-HTTP	HTTP	S/MIME	telnet, mail, news, ftp, nntp, dns, and others
	Secure Sockets Layer (SSL)		
	Transport Control Protocol		
	Internet Protocol		
	Data Link Layer		

Πίνακας 3.1: Σχέση μεταξύ υπηρεσιών δικτύων και συστημάτων πληρωμής

Οι ιδιότητες της ασφάλειας για μία συναλλαγή διαπραγματεύονται μεταξύ του πελάτη και του τροφοδότη υπηρεσιών(server) κατά τη διάρκεια της τοποθέτησης αρχικών τιμών(initialization) μιας σύνδεσης. Όταν διαπραγματεύεται, ο πελάτης ή ο server μπορούν να προσδιορίσουν αν μια συγκεκριμένη ασφαλής ιδιότητα είναι απαιτούμενη, προαιρετική ή απορριπτέα. Αν ένα συμμέτοχος καθορίσει ότι η ιδιότητα είναι απαιτούμενη, τότε αποδέχεται την σύνδεση με τον άλλο συμμέτοχο μόνο αν η ασφαλής ιδιότητα επιβαλλόμενη.

Όταν τελειώσει η διαπραγμάτευση για τις ασφαλείς ιδιότητες, το S-HTTP ασφαλίζει την σύνοδο(session) συμπυκνώνοντας τα δεδομένα μέσα σε ένα ασφαλή φάκελο. Ο φάκελος αυτός εξασφαλίζει την εμπιστευτικότητα των περιεχομένων, την ακρίβεια του μηνύματος και την αυθεντικότητα των πελατών και του server.

Εν περίληψη, το S-HTTP παρέχει στο χρήστη τη δυνατότητα να επικοινωνήσει με ασφάλεια με έναν κεντρικό υπολογιστή δικτύου με την επιλογή των επιθυμητών ασφαλών ιδιοτήτων της συναλλαγής. Και το S-HTTP και το SSL παρέχουν τη δυνατότητα να επικοινωνήσουν με ασφάλεια με τους κεντρικούς υπολογιστές δικτύου. Και οι δύο μπορούν να χρησιμοποιηθούν για να εξασφαλίσουν την εμπιστευτικότητα, την επικύρωση, και την ακεραιότητα στοιχείων. Οι προσεγγίσεις τους, εντούτοις, είναι αρκετά διαφορετικές. Επειδή η SSL κρυπτογραφεί ολόκληρη την σύνοδο(session) Διαδικτύου σε ένα στρώμα χαμηλότερου πρωτοκόλλου, μπορεί τελικά να χρησιμοποιηθεί για να εξασφαλίσει άλλες υπηρεσίες Διαδικτύου στο στρώμα εφαρμογής. Το S-HTTP υποστηρίζει μια απέραντη σειρά επιλογών για τις ασφαλείς ιδιότητες. Οι επιλογές που υποστηρίζονται καθιστούν το S-HTTP εύκαμπτο αλλά δυσκολότερο να διαμορφώθει από τον υπεύθυνο για την ανάπτυξη ιστοχώρων. Αν και η SSL έχει διάφορες επιλογές για τις ασφαλείς ιδιότητες, οι επιλογές μετατρέπονται στον browser και τους κεντρικούς υπολογιστές, καθιστώντας τη SSL ευκολότερη να χρησιμοποιήσει. Τέλος, η επικράτηση των κεντρικών υπολογιστών και των Browser Netscape στην αγορά κάνει σήμερα τη SSL την κυρίαρχη τεχνολογία για την εξασφάλιση των συνόδων ιστού(Web sessions). [1]

4. ΑΣΦΑΛΕΙΑ ΣΤΙΣ ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

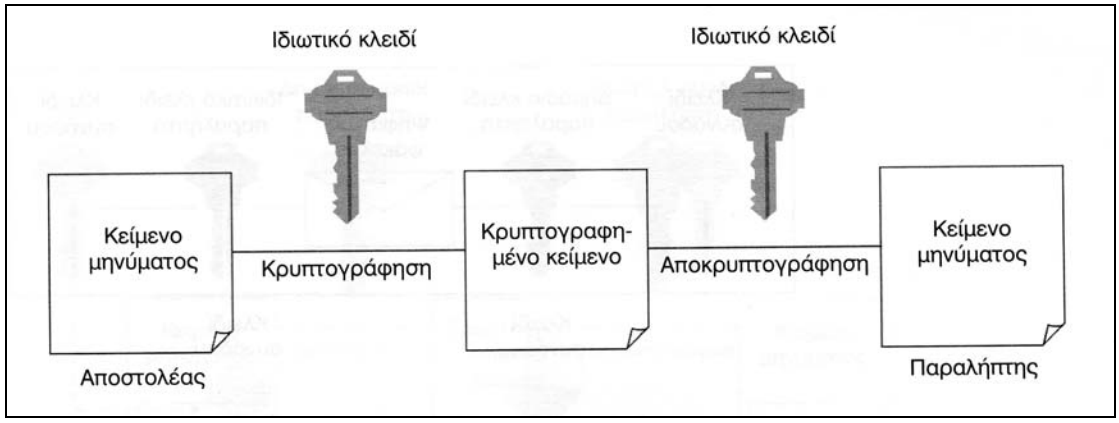
ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Ένας τρόπος για να σιγουρέψετε την εμπιστευτικότητα και το απόρρητο των μηνυμάτων είναι να βεβαιωθείτε ότι ακόμη και αν πέσει σε λάθος χέρια, δεν μπορεί να αναγνωστεί. Εδώ μπαίνει στο παιχνίδι η **κρυπτογράφηση.** Ενώ η κρυπτογράφηση είναι πολύ παλιά, (επινοήθηκε από τους αρχαίους Ελληνες), τα σημερινά συστήματα βασίζονται σε ευφυείς μαθητικούς τύπους και αλγορίθμους υπολογιστών. Ανεξάρτητα από το επίπεδο ευφυΐας, όλη η κρυπτογραφία έχει τέσσερα βασικά μέρη:

1. *Καθαρό κείμενο* - το πρωτότυπο μήνυμα σε μορφή που μπορεί να διαβάζεται από ανθρώπους.
2. *Κρυπτογραφημένο κείμενο*- το καθαρό κείμενο αφού κρυπτογραφηθεί σε μορφή που να μην μπορεί να αναγνωστεί.
3. *Αλγόριθμος κρυπτογράφησης* - ο μαθηματικός τύπος που χρησιμοποιείται για κρυπτογράφηση του καθαρού κειμένου σε κρυπτογραφημένο κείμενο και το αντίστροφο.
4. *Κλειδί* - το μυστικό κλειδί που χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση ενός μηνύματος. Διαφορετικά κλειδιά παράγουν διαφορετικό κρυπτογραφημένο κείμενο, όταν χρησιμοποιούνται με τον ίδιο αλγόριθμο.

Η κρυπτογραφία επιτρέπει την κρυπτογράφηση όχι μόνο κειμένου, αλλά επίσης και δυαδικών πληροφοριών - βίντεο, ήχου και εκτελέσιμων λειτουργικών μονάδων λογισμικού - για ασφαλή μετάδοση μέσω του Internet.

Διάφοροι αλγόριθμοι μπορούν να χρησιμοποιηθούν για κρυπτογράφηση μηνυμάτων. Ακόμη και αν ο αλγόριθμος είναι γνωστός, συνεχίζει να είναι ασφαλής αν δεν είναι γνωστό το κλειδί. Είναι δυνατό να μαντέψετε ένα κλειδί, βάζοντας απλώς ένα υπολογιστή να δοκιμάσει όλες τις πιθανότητες, μέχρι να αποκρυπτογραφηθεί το μήνυμα. Για αυτό τον λόγο το μέγεθος του κλειδιού είναι ο κύριος παράγοντας διασφάλισης ενός μηνύματος. Αν ένα κλειδί ένα μέγεθος 4 bits (π.χ., 0101), τότε θα υπάρχουν έξι πιθανότητες ($2^4 = 16$). Για κάποιο χρόνο τα κλειδιά είχαν μέγεθος 56 bits (δηλαδή $2^{36} = 72$ τετράκις εκατομμύρια πιθανότητες). Εκείνη την περίοδο οι υπολογιστές δεν ήταν σε θέση να σπάσουν το κλειδί με άσκηση μεγάλης δύναμης. Σήμερα αυτό δεν ισχύει πλέον. Οι υπολογιστές υψηλής ταχύτητας μπορούν να δοκιμάσουν εκατομμύρια συνδυασμούς σε ένα δευτερόλεπτο. Η άσκηση δύναμης επιταχύνεται επίσης από την χρήση παράλληλων επεξεργαστών, όπου ο καθένας εργάζεται σε ένα μικρότερο τμήμα των πιθανών κλειδιών. Το πραγματικό μέγεθος του κλειδιού που χρησιμοποιείται εξαρτάται από διάφορους παράγοντες. Ένας από αυτούς τους παράγοντες είναι η χρήσιμη διάρκεια ζωής των δεδομένων. Για παράδειγμα, πληροφορίες για την πιστωτική ιστορία ενός ατόμου πρέπει να παραμείνουν εμπιστευτικές πέρα από την διάρκεια της ζωής του ατόμου. Από την άλλη, ένας αριθμός πιστωτικής κάρτας πρέπει να παραμείνει εμπιστευτικός μόνο κατά την διάρκεια της ζωής της κάρτας.

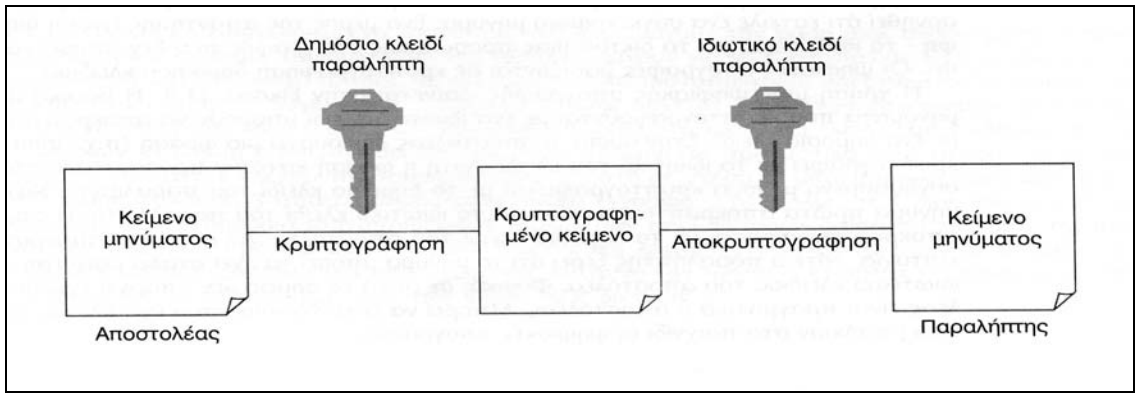


Πίνακας 4.1: Σύγχρονη κρυπτογράφηση ιδιωτικού κλειδιού

Για μεγάλο χρονικό διάστημα οι αλγόριθμοι κρυπτογράφησης ήταν συμμετρικοί, δηλαδή το ίδιο κλειδί χρησιμοποιούταν τόσο για κρυπτογράφηση, όσο και για αποκρυπτογράφηση ενός μηνύματος (Πίνακας 4.1). Αυτό σημαίνει ότι ο αποστολέας και ο παραλήπτης έπρεπε να συμφωνήσουν εκ των προτέρων για το κλειδί. Η κρυπτογράφηση συμμετρικού κλειδιού καλείται επίσης **κρυπτογράφηση ιδιωτικού κλειδιού.** Υπάρχουν πολλοί συμμετρικοί αλγόριθμοι κρυπτογράφησης. Ο ευρύτερα χρησιμοποιούμενος συμμετρικός αλγόριθμος κρυπτογράφησης ήταν ο DES, που εγκρίθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) για χρήση με αδιαβάθμητα κυβερνητικά έγγραφα. Ο DES χρησιμοποιούσε κλείδα 56-bits. Ενώ ο DES συνεχίζει να χρησιμοποιείται, άλλοι αλγόριθμοι έχουν εφευρεθεί, λόγω της ευαισθησίας του σε επιθέσεις μεγάλης δύναμης. Για παράδειγμα, οι RC2, RC4 και RC5 είναι μια σειρά αλγορίθμων κρυπτογράφησης που επινοήθηκαν από την RSA Data Security. Τα κλειδιά τους έχουν μέγεθος μέχρι 2048 bits.

Μια δυσκολία με την κρυπτογράφηση συμμετρικού ή ιδιωτικού κλειδιού είναι ότι πολλά μηνύματα του Internet στέλνονται ανάμεσα σε άτομα ή άτομα και μηχανήματα που δεν έχουν συναντηθεί ποτέ. Αν το ιδιωτικό κλειδί ενός server διανεμηθεί σε χιλιάδες χρήστες, δεν υπάρχει τρόπος το κλειδί να παραμείνει μυστικό για πολύ χρόνο. Για αυτούς τους λόγους, ένας νέος τύπος αλγορίθμου, που καλείται κρυπτογράφηση δημόσιου κλειδιού, επινοήθηκε το 1976 από τους Whitfield και Martin Hellmann.

Η κρυπτογράφηση δημόσιου κλειδιού, επίσης γνωστή σαν ασύμμετρη κρυπτογράφηση, χρησιμοποιεί ένα ζεύγος κλειδιών - ένα δημόσιο και ένα ιδιωτικό. Το δημόσιο κλειδί γίνεται γνωστό σε όλους όσους θέλουν να στείλουν ένα κρυπτογραφημένο μήνυμα στον κάτοχο του ιδιωτικού κλειδιού. Ο μόνος τρόπος αποκρυπτογράφησης του μηνύματος είναι με το ιδιωτικό κλειδί. Με αυτό τον τρόπο, μηνύματα μπορούν να σταλούν χωρίς εκ των προτέρων συμφωνία για τα κλειδιά. Η διαδικασία **κρυπτογράφησης δημόσιου κλειδιού** φαίνεται διαγραμματικά στον Πίνακα 4.2.[5]

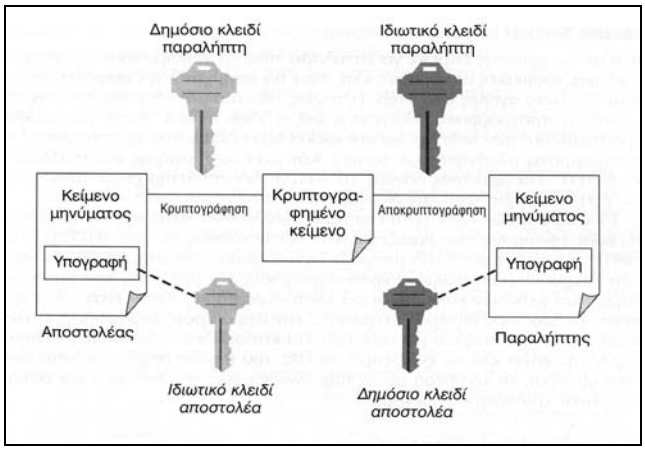


Πίνακας 4.2: Κρυπτογράφηση Δημόσιου κλειδιού

ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ

Πώς μπορείτε να είστε σίγουροι ότι ένα μήνυμα έρχεται πραγματικά από το άτομο που νομίζετε ότι έρχεται; Επίσης, πώς μπορείτε να είστε σίγουρος ότι ένα άτομο δεν έχει κανένα τρόπο να αρνηθεί ότι έστειλε ένα συγκεκριμένο μήνυμα; Ένα μέρος της απάντησης είναι η **«ψηφιακή υπογραφή»** - το ισοδύναμο για τα δίκτυα μιας προσωπικής υπογραφής που δεν μπορεί να πλαστογραφηθεί . Οι ψηφιακές υπογραφές βασίζονται σε κρυπτογράφηση δημόσιου κλειδιού.

Η χρήση μιας ψηφιακής υπογραφής φαίνεται στον Πίνακα 4.3. Η βασική ιδέα είναι ότι τα μηνύματα που κρυπτογραφούνται με ένα ιδιωτικό κλειδί μπορούν να αποκρυπτογραφηθούν μόνο με ένα δημόσιο κλειδί. Στην ουσία, ο αποστολέας δημιουργεί μια φράση (π.χ., John J.Jones) και την κρυπτογραφεί με το ιδιωτικό του κλειδί. Αυτή η φράση κατόπιν προσαρτάται στο μήνυμα και το συνδυασμένο μήνυμα κρυπτογραφείται με το δημόσιο κλειδί του παραλήπτη. Κατά την λήψη, το μήνυμα πρώτα αποκρυπτογραφείται με το ιδιωτικό κλειδί του παραλήπτη. Η φράση υπογραφής αποκρυπτογραφείται με το δημόσιο κλειδί του αποστολέα. Αν η φράση αποκρυπτογραφηθεί με επιτυχία, τότε ο παραλήπτης ξέρει ότι το μήνυμα μπορεί να έχει σταλεί μόνο από τον κάτοχο το ιδιωτικού κλειδιού του αποστολέα. Φυσικά, σε αυτό το σημείο δεν υπάρχει εγγύηση ότι ο αποστολέας είναι πραγματικά ο αποστολέας. Μπορεί να είναι κάποιος που έχει κλέψει το ιδιωτικό κλειδί. Εδώ μπαίνουν στο παιχνίδι οι ψηφιακές υπογραφές.[5]



Πίνακας 4.3: Ψηφιακή υπογραφή

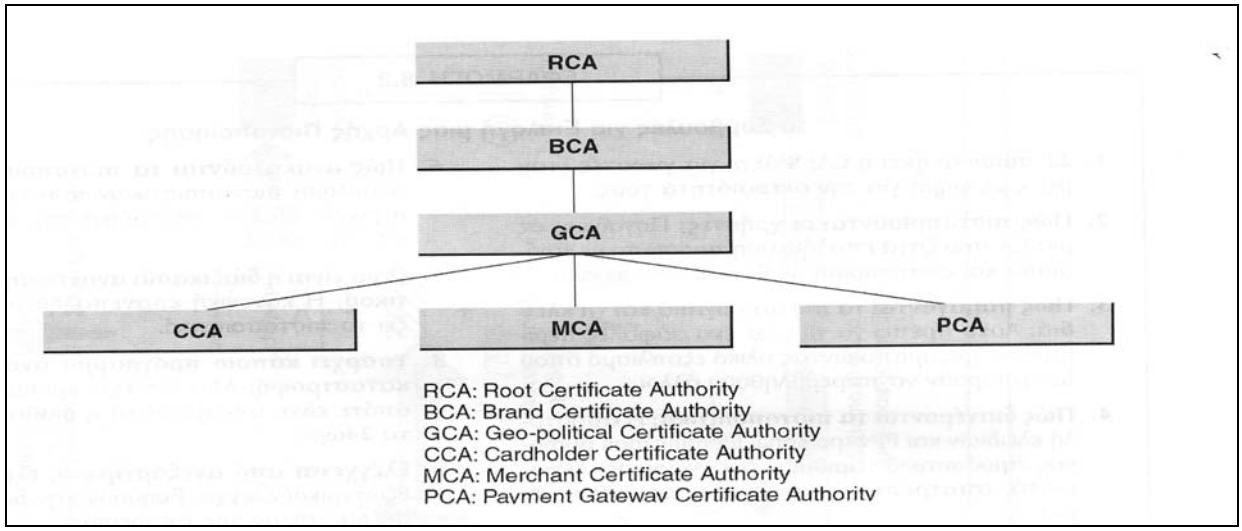
ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

Ας υποθέσουμε ότι παίρνω το δημόσιο κλειδί κάποιου φίλου για παράδειγμα του Πάνου από κάποιον κατάλογο online, ώστε να το χρησιμοποιώ για να του στέλνω κρυπτογραφημένα μηνύματα, τα οποία μόνο εκείνος θα μπορεί να διαβάζει (αφού μόνο εκείνος έχει το αντίστοιχο μυστικό κλειδί). Πώς, όμως, μπορώ να είμαι βέβαιος ότι το κλειδί που πήρα όντως ανήκει στον Πάνο; Διότι, εάν υποθέσουμε ότι ένας κράκερ γνωρίζει τα στοιχεία του Πάνου, τότε ίσως έχει βάλει το δικό του δημόσιο κλειδί στη θέση του Πάνου. Κάθε φορά, λοιπόν, που εγώ θα στέλνω ένα e-mail στη διεύθυνση panos@somewhere.net, ο κράκερ θα μπορεί να υποκλέπτει και να το διαβάζει, αφού στην ουσία θα το έχω κρυπτογραφήσει με το δικό του δημόσιο κλειδί.

Το ηθικό δίδαγμα που προκύπτει είναι 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 δ*2* στο χρήστη *χ2* κ.λ.π. Συνήθως, η αντιστοίχηση ενός χρήστη στο δημόσιο κλειδί του παρέχεται από ένα πιστοποιητικό (certificate). Τα πιστοποιητικά διανέμει η λεγόμενη Αρχή Πιστοποίησης [Certification Authority ή CA), που δεν είναι τίποτα άλλο από έναν έμπιστο οργανισμό ή μια εταιρεία. Μια τέτοια Αρχή έχει την ευθύνη της δημιουργίας, της διανομής, της ανάκλησης και γενικά της διαχείρισης των πιστοποιητικών.

Έτσι, εάν ο Πάνος επιθυμεί ένα πιστοποιητικό, αρχικά θα απευθυνθεί σε μια Αρχή Πιστοποίησης, όπως είναι η Verisign (http://www.verisign.com/). Η Αρχή θα ελέγξει με κάποιον τρόπο την ταυτότητα του Πάνου, καθώς και ότι το δημόσιο κλειδί δ που προσκομίζει του ανήκει πραγματικά. Ακολουθεί η σύνταξη ενός κειμένου, το οποίο θα περιλαμβάνει στοιχεία που αφορούν στον Πάνο (π.χ., ονοματεπώνυμο, διεύθυνση κατοικίας, e-mail κ.λ.π.), το κλειδί *δ,* καθώς και άλλα χρήσιμα στοιχεία, όπως, π.χ., η ημερομηνία κατά την οποία η ισχύς του πιστοποιητικού εκπνέει (expiration date). Στη συνέχεια, η Αρχή Πιστοποίησης υπογράφει το έγγραφο με το δικό της μυστικό κλειδί, δημιουργώντας έτσι το πιστοποιητικό του Πάνου. Τώρα, εάν εγώ θέλω το δημόσιο κλειδί του Πάνου, καθώς και να επιβεβαιώσω ότι είναι δικό του, τότε παίρνω πρώτα το πιστοποιητικό του Πάνου από έναν κατάλογο online. Επαληθεύω την ψηφιακή υπογραφή της Αρχής Πιστοποίησης και αν είναι εντάξει, είμαι πλέον βέβαιος ότι το κλειδί που πήρα πράγματι ανήκει στον Πάνο. Τέλος, ο λόγος για τον οποίο οι χρήστες εμπιστεύονται μια κάποια Αρχή Πιστοποίησης έγκειται, συνήθως, στο γεγονός ότι κάποιος άλλος φορέας εγγυάται για την αξιοπιστία της. Για τον τελευταίο φορέα μπορεί να εγγυάται κάποιος άλλος κ.λ.π. Έχουμε, λοιπόν, μια αλυσίδα εμπιστοσύνης (chain of trust), στη ρίζα της οποίας (root) υπάρχει μια καθολικά αποδεκτή Αρχή.[2]

Πίνακας 4.4: Ένα επεξηγηματικό πιστοποιητικό



Πίνακας 4.5: Ιεραρχία Αρχών Πιστοποίησης

ΣΥΓΚΡΙΣΗ PKI (Public Key Infrastructure) ΚΑΙ IPSec

PKI

Η *υποδομή δημόσιου κλειδιού* (Public Key Infrastructure-PKI) είναι μια βάση ασφαλείας που βεβαιώνει ότι οι συναλλαγές μέσω του Web μπορεί να είναι αξιόπιστες, όπως ήταν οι προσωπικές συναλλαγές κάποτε. Το PKI αποτελείται από τέσσερα διαφορετικά μέρη που δουλεύουν μαζί για να δημιουργήσουν τη βάση ασφαλείας:

- Κρυπτογράφηση δημόσιου κλειδιού
- Ψηφιακή υπογραφή
- Αρχή Έκδοσης Πιστοποιητικών (Certificate Authority – CA)
- Αρχή Έκδοσης Εγγράφων (Registration Authority – RA)

Κρυπτογράφηση Δημοσίου Κλειδιού

Η βάση του PKI είναι μία τεχνολογία που ονομάζεται κρυπτογράφηση δημόσιου κλειδιού. Η *κρυπτογράφηση δημόσιου κλειδιού* (public key cryptography), είναι η τεχνολογική λύση στο πρόβλημα που δημιουργείται από τα άτομα που υποκλέπτουν τα εμπιστευτικά μηνύματα που στέλνονται μέσω του Internet. Είναι ένας μαθηματικός μυστικός κώδικας με τον οποίο κάθε γράμμα αλλάζει σε ένα διαφορετικό γράμμα, αριθμό ή σύμβολο, δημιουργώντας μία σελίδα που δεν έχει έννοια, ώστε το μήνυμα να μην μπορεί να διαβαστεί, ακόμα και αν υποκλαπεί.

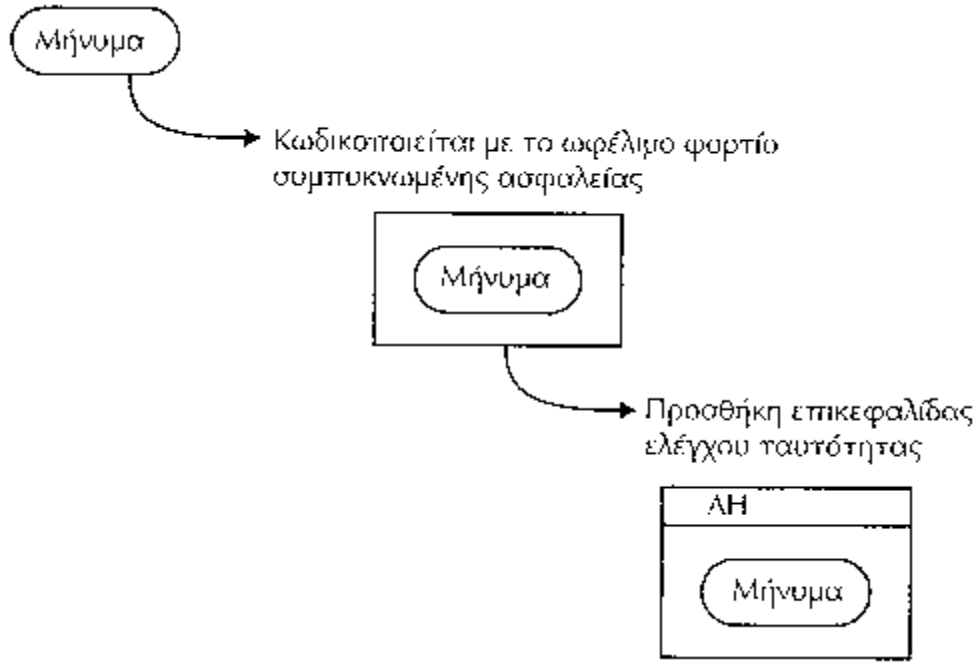
Η κρυπτογράφηση του δημόσιου κλειδιού είναι διαφορετική από τον ιστορικό μυστικό κώδικα και χρησιμοποιείται μέσω του Internet επειδή έχει δύο κλειδιά. Δημιουργείται από ένα μαθηματικό κώδικα που βασίζεται σε ένα αλγόριθμο και σε μία τιμή, με ένα συμπληρωματικό αλγόριθμο και τιμή. Η εξυπνάδα αυτού του συστήματος είναι ότι ο ένας αλγόριθμος μπορεί να κρυπτογραφήσει το μήνυμα και ο άλλος να το αποκρυπτογραφήσει. Συνεπώς, ο ένας από τους δύο αλγόριθμους μπορεί να γίνει δημόσιος ενώ ο άλλος κρατιέται μυστικός. Είναι αδύνατο για ένα άτομο να αποκρυπτογραφήσει το ιδιωτικό κλειδί από το δημόσιο κλειδί ή το αντίστροφο. Με αυτό το σύστημα κρυπτογράφησης, δεν έχει σημασία εάν ο κώδικας υποκλέπτεται και διαβάζεται, επειδή είναι δημόσιος. Ο μόνος κώδικας που μπορεί να αποκρυπτογραφήσει τα κρυπτογραφημένα μηνύματα είναι αυτός που παραμένει ιδιωτικός.

IPSec

Το IPSec λειτουργεί κλείνοντας το πακέτο των πληροφοριών το οποίο στέλνεται, σε ένα άλλο πακέτο, πριν σταλεί μέσω του Internet. Στον παραλήπτη, το

πακέτο αποκωδικοποιείται και διαβάζεται από μια συσκευή που έχει καθορίσει ο αποστολέας.

Το IPSec αποτελείται από τρεις διαφορετικούς μηχανισμούς ασφαλείας: την επικεφαλίδα ελέγχου ταυτότητας, το ωφέλιμο φορτίο συμπυκνωμένης ασφάλειας και το κλειδί διαχείρισης. Οι τρεις μηχανισμοί χρησιμοποιούνται σε συνδυασμό μεταξύ τους, για καλύτερα αποτελέσματα ασφαλείας.



Επικεφαλίδα ελέγχου ταυτότητας

Ο πρώτος μηχανισμός είναι η *επικεφαλίδα ελέγχου ταυτότητας* (authentication header – AH). Το AH επικεντρώνεται στον έλεγχο ταυτότητας των ατόμων που στέλνουν τις πληροφορίες και βεβαιώνεται ότι δεν έχουν αλλοιωθεί στη διαδρομή. Το AH μπαίνει μετά στην IP επικεφαλίδα, αλλά πριν από τις άλλες πληροφορίες που πρόκειται να πιστοποιηθούν.

Ωφέλιμο φορτίο συμπυκνωμένης ασφάλειας

Ο δεύτερος μηχανισμός είναι το *ωφέλιμο φορτίο συμπυκνωμένης ασφάλειας* (encapsulating security payload – ESP). Το ESP πιστοποιεί επίσης την ταυτότητα του χρήστη, αλλά υποστηρίζει και την κρυπτογράφηση των δεδομένων.

Πρωτόκολλο διαχείρισης κλειδιού Internet

Το Πρωτόκολλο διαχείρισης κλειδιού Internet (Internet Key Management Protocol) λέγεται ότι είναι ο πυρήνας του IPSec. Αυτός ο μηχανισμός επιτρέπει να ανταλλάσσουν δύο μέρη τα δημόσια κλειδιά τους και να διαμορφώνουν μια ασφαλή σύνοδο. Αφού ανταλλαχθούν τα δημόσια κλειδιά, ορίζεται ένα προσδιοριστικό συνόδου. Ένα *προσδιοριστικό συνόδου (session identifier)* είναι ο ορισμός της Internet σχέσης που μοιράζονται τα δύο μέρη.

Το IPSec είναι όπως το PKI στο τρόπο που ορίζει την εμπιστοσύνη μεταξύ διαφορετικών πλευρών. Σαν καθολική βάση, το IPSec παρέχει τρεις πολύ σημαντικές λειτουργίες ασφαλείας για Internet συναλλαγές: εμπιστοσύνη, ακεραιότητα και έλεγχο ταυτότητας.

Εμπιστοσύνη Το IPSec βεβαιώνεται ότι όλες οι συναλλαγές είναι εμπιστευτικές, με τον ίδιο τρόπο που το κάνει ο μηχανισμός PKI. Η λειτουργία ESP κρυπτογραφεί τα πακέτα πριν σταλούν μέσω του Internet. Αφού κρυπτογραφηθεί η συναλλαγή, μπορεί μόνο να αποκρυπτογραφηθεί από το Web διακομιστή. Έτσι, ακόμα και αν οι πληροφορίες υποκλαπούν, δεν θα μπορούσαν να αποκρυπτογραφηθούν.

Ακεραιότητα Ο παραλήπτης, σε αυτή τη περίπτωση ο Web διακομιστής, μπορεί επίσης να βεβαιωθεί ότι τα δεδομένα δεν έχουν αλλαχθεί ή υποκλαπεί με κάποιον τρόπο. Επειδή η συναλλαγή κρυπτογραφείται πριν σταλεί, θα αποκρυπτογραφηθεί αν το μήνυμα δεν αλλοιωθεί. Έτσι, αν υπάρχει κάποια αλλαγή στο μήνυμα, δεν θα μεταφραστεί σε αναγνώσιμο υλικό όταν φτάσει στο Web διακομιστή.
Έλεγχος ταυτότητας Ο παραλήπτης μπορεί επίσης να πιστοποιήσει την πηγή από την οποίαν προέρχονται τα πακέτα, εξ αιτίας των πληροφοριών που παρέχονται στην επικεφαλίδα.

Διαφορές από το PKI

Αν και το IPSec ακούγεται πολύ παρόμοιο με την προσέγγιση PKI για την οποία συζητήσαμε στο τελευταίο κεφάλαιο, υπάρχει από την αρχή μία πολύ βασική διαφορά. Τα άλλα μέτρα ασφαλείας συναλλαγών που έχουμε δει λειτουργούν σε επίπεδο εφαρμογής, ενώ το IPSec λειτουργεί σε επίπεδο πρωτοκόλλου. Αυτό κάνει το IPSec ευκολότερο στη χρήση, επειδή οι εφαρμογές των δύο πλευρών που επικοινωνούν δεν χρειάζεται να είναι συμβατές. Επιπλέον, το IPSec επιτρέπει στους χρήστες να πιστοποιούν και να επικοινωνούν μέσω μίας σύνδεσης, αντί να επικοινωνούν με μηνύματα. Το PKI είναι ένα θαυμάσιο μέτρο ασφαλείας για μηνύματα ηλεκτρονικού ταχυδρομείου. Το IPSec είναι πιο κατάλληλο για χρήση στο Internet.[4]

5. ΑΣΦΑΛΕΙΑ ΣΤΑ ΗΛΕΚΤΡΟΝΙΚΑ ΣΥΣΤΗΜΑΤΑ ΠΛΗΡΩΜΩΝ

SECURE SOCKET LAYER (SSL)

Αν ο μέσος χρήστης έπρεπε να καταλάβει πώς να χρησιμοποιεί κρυπτογράφηση, ψηφιακά πιστοποιητικά, ψηφιακές υπογραφές κλπ, τότε θα υπήρχαν λίγες ασφαλείς συναλλαγές και συνεπώς θα γίνονταν λίγες αγορές στο Web. Ευτυχώς, όλα αυτά τα θέματα τα διαχειρίζονται με ένα διαφανή τρόπο τα προγράμματα πλοήγησης και οι Web servers. Αυτό γίνεται κυρίως μέσω ενός ειδικού πρωτοκόλλου, που καλείται **secure socket layer (SSL)**, που κρυπτογραφεί επικοινωνίες ανάμεσα σε προγράμματα πλοήγησης και servers. Κάποια εποχή υπήρχε ένα εναλλακτικό πρωτόκολλο με όνομα S-HTTP. Για αρκετούς λόγους το S-HTTP δεν υποστηρίχτηκε πολύ. Σήμερα, η έκδοση 3.0 του SSL έχει υιοθετηθεί από την Netscape και από την Microsoft.

Το secure socket layer είναι ένα πρωτόκολλο που λειτουργεί στο επίπεδο TCP/IP. Αυτό σημαίνει ότι κάθε εφαρμογή που βασίζεται στο TCP/IP - όπως το Web (HTTP), οι ομάδες ειδήσεων UseNet (NNTP), και το e-mail (SMTP) μπορούν να διασφαλιστούν από το SSL. Το secure socket layer υποστηρίζει διάφορους αλγόριθμους κρυπτογράφησης και μεθόδους πιστοποίησης. Ο συνδυασμός αλγορίθμων και μεθόδων καλείται *σειρά* κρυπτογράφησης. Οταν ένας πελάτης έρχεται σε επαφή με ένα server, οι δύο τους διαπραγματεύονται την σειρά κρυπτογράφησης, επιλέγοντας την δυνατότερη σειρά που είναι κοινή και για τους δύο. Για ιστοσελίδες, η διαδικασία διαπραγμάτευσης ξεκινά όταν ο χρήστης κάνει κλικ σε ένα δεσμό, το URL του οποίου αρχίζει με https αντί του http (π.χ., https:// www.ups.com,/ σε αντίθεση με το http://www.ups.com/). Από εκεί και ύστερα, όλες οι επικοινωνίες τους είναι κρυπτογραφημένες.

Ασφάλεια

Ο μεγαλύτερος κίνδυνος ασφαλείας με το Secure Sockets Layer είναι ότι οι έμποροι που χρησιμοποιούν το πρωτόκολλο πρέπει να κρατήσουν τους servers ασφαλείς έτσι ώστε οι αριθμοί πιστωτικών καρτών να παραμείνουν ασφαλείς. Κατά

συνέπεια ο πελάτης πρέπει να εμπιστευθεί όχι μόνο τον έμπορο και τους υπαλλήλους του, αλλά και την διορατικότητα του τεχνικού στην ασφάλεια υπολογιστών. Η κλοπή 20.000 αριθμών πιστωτικών καρτών από την Netcom στις αρχές της δεκαετίας του '90 διευκρινίζει ότι η επέκταση αυτής της εμπιστοσύνης είναι μια προβληματική πρόταση. Εάν οι υπάλληλοι ενός εμπόρου είναι ανέντιμοι, οι οργανωτικές διαδικασίες ασφάλειάς του ανεπαρκείς, ή η εγκατάσταση του λογισμικού του ελαττωματικού, ο καταναλωτής διατρέχει τον κίνδυνο για την απάτη πιστωτικών καρτών.

Ακόμα κι αν ο έμπορος είναι τίμιος, οι υπάλληλοί του μπορούν να παρουσιάσουν ένα πρόβλημα ασφάλειας. Οι επανειλημμένες επιθέσεις είναι εύκολο να ξεκινήσουν για έναν ανέντιμο υπάλληλο που δεν έχει την πρόσβαση στις πληροφορίες που παρέχονται στον έμπορο.

Μυστικότητα

Το Secure Sockets Layer μπορεί να μην παρέχει οικονομικές υπηρεσίες, αλλά σίγουρα προσφέρει το λογισμικό για να δημιουργήσει μια κάποιος μια εξασφαλισμένη κρυπτογράφηση για σύνδεση μέσω του Διαδικτύου. Η μη απευθείας σύνδεση με τράπεζα είναι ο οικονομικός φορέας παροχής υπηρεσιών, και ο Netscape είναι μόνο ο προμηθευτής λογισμικού ασφάλειας μετάδοσης, δεν παρέχει κανένα κρυπτογραφικό πιστοποιητικό και δεν παρέχει καμία έγκριση οικονομικής συναλλαγής. Ο Netscape δεν λαμβάνει ούτε διατηρεί οποιεσδήποτε πληροφορίες για οποιαδήποτε συναλλαγή που διευθύνεται χρησιμοποιώντας το Secure Sockets Layer.

Ο πίνακας 5.1 παρουσιάζει τις διαθέσιμες πληροφορίες για τα διάφορα συμβαλλόμενα μέρη σε μια συναλλαγή που χρησιμοποιεί το Secure Sockets Layer. Η πληροφορία ταυτότητας(identity information) είναι διαθέσιμη όπως άλλωστε φαίνεται στον πίνακα 5.1 διότι τα πιστοποιητικά για την πιστοποίηση του καταναλωτή και του εμπόρου στέλνονται χωρίς κρυπτογράφηση.

	Information				
Party	Merchant	Customer	Date	Amount	Item
Merchant	Full	Full	Full	Full	Full
Customer	Full	Full	Full	Full	Full
Law enforcement with warrant	Full	Full	Full	Full	Full
Netscape	None	None	None	None	None
Bank	Full	Full	Full	None	Full
Observer	Full	Full	Full*	None	None

** Ο παρατηρητής μπορεί να αποφασίσει μόνο όταν η επικοινωνία έγινε μεταξύ εμπόρου και καταναλωτή*

Πίνακας 5.1: Διαθέσιμες πληροφορίες στα συμβαλλόμενα μέρη σε μια συναλλαγή που χρησιμοποιεί SSL

Διοίκηση

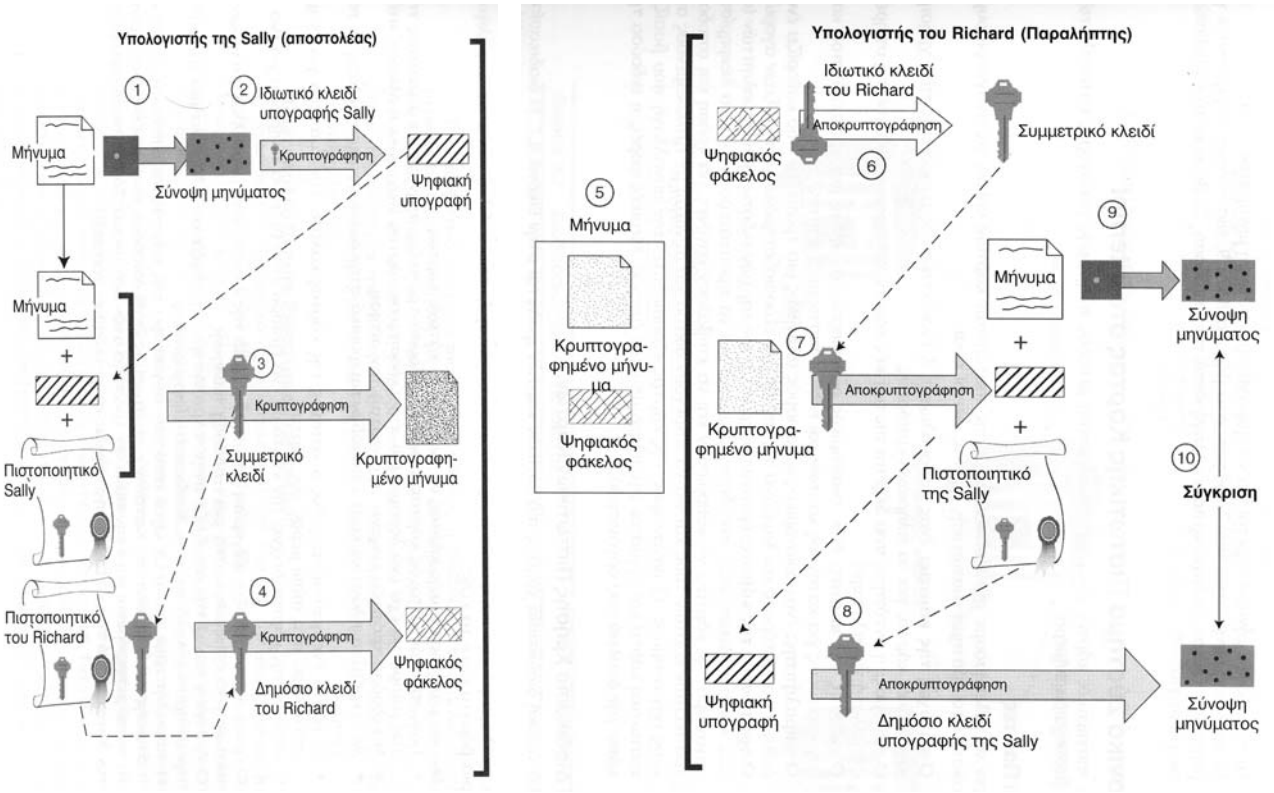
Το Secure Sockets Layer φτιάχνει ασφαλείς συνδέσεις μέσω ενός ανοικτού δικτύου. Ο Netscape σαν μία οντότητα δεν έχει καμία πληροφορία για το ποια δεδομένα έχουν περάσει μέσα από μια ασφαλή Sockets σύνδεση, έτσι δεν υπάρχει κεντρική αποθήκη πληροφοριών για διοίκηση.

Σχήματα ασφάλειας υιοθετούνται σε πρωτόκολλα σαν το SSL και το SET. Αυτή η ενότητα εξηγεί το πρωτόκολλο γενικής χρήσης SSL. Το SET, προσαρμοσμένο για

πληρωμές πιστωτικής κάρτας στο Internet, θα εξηγηθεί στην επόμενη ενότητα. Επειδή το SET έχει καθοριστεί επάνω στο SSL, η κατανόηση του SSL είναι η βάση για την κατανόηση του 5ET. Το πρωτόκολλο Secure-HTTP (S-HTTP) εφαρμόζει το SSL ανάμεσα σε Web servers και σε προγράμματα πλοήγησης, που επικοινωνούν με το πρωτόκολλο HTTP.

Το πρωτόκολλο SSL κάνει ανταλλαγή μηνυμάτων όπως φαίνεται στον Πίνακα 5.2. Υποθέστε ότι ο αποστολέας είναι η Sally και ο παραλήπτης είναι ο Richard. Τα βήματα της διαδικασίας αντιστοιχούν στους αριθμούς στην Πίνακα 5.2.

1. Στον δικτυακό τόπο της Sally, το μήνυμα προς αποστολή κόβεται στο προηγουμένως σταθερό μήκος για σύνοψη μηνύματος.
2. Η σύνοψη μηνύματος κρυπτογραφείται με το κλειδί ιδιωτικής υπογραφής της Sally χρησιμοποιώντας ένα αλγόριθμο RSA, και η έξοδος είναι μια ψηφιακή υπογραφή.
3. Η ψηφιακή υπογραφή και το πιστοποιητικό της Sally προσαρτώνται στο αρχικό μήνυμα. Στο μεταξύ, ένα μυστικό κλειδί, που χρησιμοποιεί τον αλγόριθμο DES στον υπολογιστή της Sally, κρυπτογραφεί την δέσμη με το κλειδί.
4. Το συμμετρικό κλειδί κρυπτογραφείται με το δημόσιο κλειδί του Richard, που βρίσκεται στο πιστοποιητικό του Richard, το οποίο έχει ληφθεί εκ των προτέρων. Το αποτέλεσμα είναι ένας ψηφιακός φάκελος.
5. Το κρυπτογραφημένο μήνυμα και ο ψηφιακός φάκελος μεταδίδονται στον υπολογιστή του Richard μέσω του Internet.
6. Ο ψηφιακός φάκελος αποκρυπτογραφείται με το ιδιωτικό κλειδί ανταλλαγής του Richard.
7. Χρησιμοποιώντας το επαναφερθέν μυστικό κλειδί, το παραληφθέν μήνυμα αποκρυπτογραφείται στο μήνυμα, στην ψηφιακή υπογραφή και στο πιστοποιητικό της Sally.
8. Για επιβεβαίωση της ακεραιότητας, η ψηφιακή υπογραφή αποκρυπτογραφείται από το δημόσιο κλειδί της Sally (που βρίσκεται στο πιστοποιητικό της Sally), λαμβάνοντας την σύνοψη μηνύματος.[3,5]



Πίνακας 5.2: Σχήματα ασφαλούς μετάδοσης στα πρωτόκολλα SSL και SET

SECURE ELECTRONIC TRANSACTIONS (SET)

Το SSL. κάνει δυνατή την κρυπτογράφηση αριθμών πιστωτικών καρτών που στέλνονται από το πρόγραμμα πλοήγησης ενός καταναλωτή στον δικτυακό τόπο ενός εμπόρου. Υπάρχουν όμως πολύ περισσότερα πράγματα όταν γίνεται μια αγορά στο Web από το απλό πέρασμα ενός αριθμού πιστωτικής κάρτας σε ένα έμπορο. Ο αριθμός πρέπει να ελεγχθεί για την εγκυρότητα του, η τράπεζα του καταναλωτή πρέπει να εξουσιοδοτήσει την κάρτα, και πρέπει να γίνει η επεξεργασία της αγοράς. Το SSL δεν έχει σχεδιαστεί να διαχειρίζεται κανένα από αυτά τα βήματα, πέρα από την μετάδοση του αριθμού της κάρτας. Ένα πρωτόκολλο κρυπτογράφησης που έχει σχεδιαστεί για να χειρίζεται την πλήρη συναλλαγή είναι το **secure electronic transaction (SET)**, που έχει αναπτυχθεί από κοινού από τις Visa, Mastercard , Netscape και Microsoft. Το πρωτόκολλο SET παρέχει πιστοποίηση, εμπιστευτικότητα, ακεραιότητα μηνύματος και σύνδεση, βασίζεται σε δημόσια και ιδιωτικά κλειδιά για τον καταναλωτή και τον έμπορο και υποστηρίζει τα παρακάτω χαρακτηριστικά (Stein 1998):

- εγγραφή κατόχου κάρτας
- εγγραφή εμπόρου
- αιτήσεις αγοράς
- εξουσιοδότηση πληρωμής
- σύλληψη πληρωμής
- επιστροφές χρεώσεων
- πιστώσεις
- αντιστροφή πίστωσης
- συναλλαγές χρεωστικής κάρτας

Τα μόνα εμπορικά προϊόντα που παρέχουν σήμερα συναλλαγές SET είναι η εφαρμογή Wallet της Verifone Corporation για καταναλωτές και η επέκταση vPOS για τον Merchant Web Server της Microsoft. Στο μέλλον, τα προγράμματα πλοήγησης της Netscape και της Microsoft θα παρέχουν υποστήριξη για SET.

Ασφάλεια

Η πιο δραματική βελτίωση του Secure Electronic Transaction Protocol πέρα από το πρωτόκολλο διαταγής τηλεφώνων και ταχυδρομείου για Mastercard είναι ότι ο έμπορος παίρνει μόνο αρκετές πληροφορίες για μόνο μια αγορά. Οι έμποροι δεν μπορούν να χρησιμοποιήσουν το Secure Electronic Transaction Protocol για τις επαναλαμβανόμενες επιθέσεις.

Το Secure Electronic Transaction Protocol δεν περιλαμβάνει διαπραγμάτευση ή εξακρίβωση της παράδοσης της πληροφορίας αγαθών. Η μη αποποίηση της ευθύνης έχει περιορισμένη δύναμη όταν η υπόσχεση μπορεί να εξακριβωθεί αλλά η ολοκλήρωση της υπόσχεσης δεν μπορεί.

Η έλλειψη ατομικότητας των αγαθών που διέπει το Secure Electronic Transaction Protocol δημιουργεί εύφορο έδαφος για απάτες. Επίσης το πρωτόκολλο αυτό εμπεριέχει την δυνατότητα χρησιμοποίησης ψευδωνύμου όσον αφορά τον αριθμό λογαριασμού.

Η διεύθυνση του καταναλωτή(customer) και τα δεδομένα παραγγελίας προσφέρονται στους εμπόρους(merchants) σε ένα ξεχωριστό κανάλι από το Secure Electronic Transaction Protocol μέσω των πελατών. Γι' αυτό το λόγο αυτή η πληροφορία είναι διαθέσιμη στους παρατηρητές(observers).

Μυστικότητα

Ο Πίνακας 5.3 παρουσιάζει τις διαθέσιμες πληροφορίες σε μια συναλλαγή χρησιμοποιώντας το Secure Electronic Transaction Protocol.

Το ασφαλές ηλεκτρονικό πρωτόκολλο συναλλαγής(Secure Electronic Transaction Protocol) παρέχει περισσότερη μυστικότητα από τις τυποποιημένες συναλλαγές πιστωτικών καρτών έξω από το Διαδίκτυο, δεδομένου ότι ο πελάτης μπορεί να επιλέξει έναν ψευδώνυμο αριθμό λογαριασμού. Αυτό υπονοεί ότι η ικανότητα για τη χρησιμοποίηση των ψευδωνύμων χτίζεται στο ασφαλές ηλεκτρονικό πρωτόκολλο συναλλαγής, αν και δεν είναι την συγκεκριμένη στιγμή σαφής. Σημειώστε ότι το γεγονός ότι οι οικονομικές πληροφορίες είναι κρυμμένες από την έμπορο αυξάνει την ασφάλεια και όχι την μυστικότητα.

Ένας ηλεκτρονικός παρατηρητής μπορεί να λάβει την πλήρη γνώση για μια συναλλαγή χρησιμοποιώντας το ασφαλές ηλεκτρονικό πρωτόκολλο συναλλαγής επειδή τα πιστοποιητικά που περιέχουν τις πληροφορίες ταυτότητας των συμβαλλόμενων μερών συναλλαγής διαβιβάζονται εκτός(in the clear).

	Information				
Party	Merchant	Customer	Date	Amount	Item
Merchant	Full	Partial	Full	Full	Full
Customer	Full	Full	Full	Full	Full
Law enforcement with warrant	Full	Full	Full	Full	Full
Bank	Full	Full	Full	Full	Full
Observer	Full	Full	Full	Full	Full

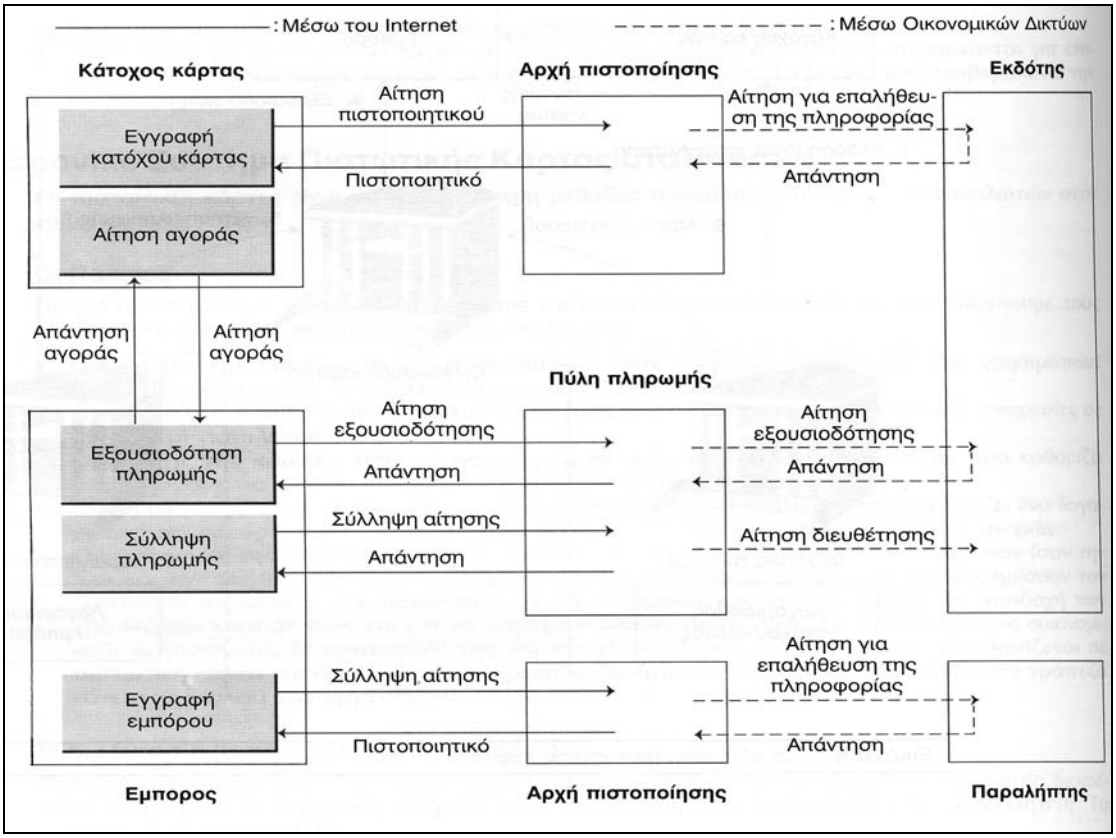
Πίνακας 5.3: Διαθέσιμες πληροφορίες στα συμβαλλόμενα μέρη σε μια συναλλαγή πρωτοκόλλου SET

Διοίκηση

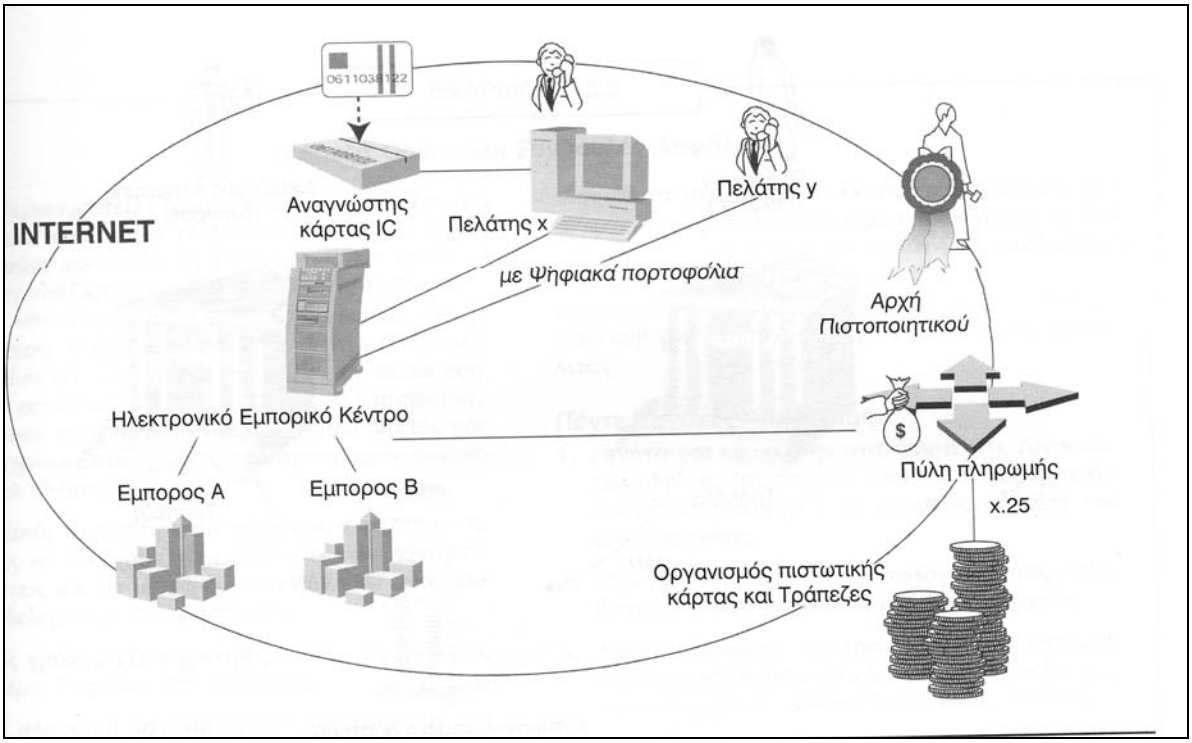
Το Secure Electronic Transaction Protocol είναι ένα ανοικτό πρότυπα που παρέχει όλες τις απαραίτητες πληροφορίες για ρυθμιστικούς λόγους. Το Secure Electronic Transaction Protocol δεν βελτιστοποιείται πρώτιστα για τη μυστικότητα δεδομένου ότι το όνομα και η διεύθυνση του πελάτη απαιτούνται από τον έμπορο για την επαλήθευση. Με τη χρήση των πιστοποιητικών και των δημόσιων κλειδιών, το πλεονέκτημα ασφάλειας που αποκομίζεται με την απαίτηση του συνυπολογισμού τέτοιων πληροφοριών είναι αμφισβητήσιμο για τα στοιχεία που δεν απαιτούν τη φυσική παράδοση. Στην πραγματικότητα, η χρήση ενός πιστοποιητικού με ψευδώνυμο χωρίς τις φυσικές πληροφορίες πελατών δεν θα απαιτούσε καμία αλλαγή στα πρωτόκολλα και θα πρόσφερε μια απέραντη βελτίωση στην καταναλωτική ιδιωτικότητα.

Το *SET* ορίζει την μορφή του μηνύματος, την μορφή του πιστοποιητικού και την διαδικασία της ανταλλαγής μηνύματος, όπως παρουσιάζεται στην Εικόνα 5.4.
Στο πρωτόκολλο SET, υπάρχουν τέσσερις οντότητες: κάτοχος κάρτας, έμπορος, αρχή πιστοποίησης (Certificate Authority-CA) και πύλη πληρωμής, όπως φαίνεται στην Εικόνα 5.5. Οι ρόλοι του εκδότη, του παραλήπτη και του οργανισμού είναι πέρα από τις προδιαγραφές του πρωτοκόλλου SET. Ο ρόλος της πύλης πληρωμής είναι να συνδέει το Internet με τα ιδιωτικά δίκτυα τραπεζών. Κάθε συμμετέχουσα οντότητα χρειάζεται το δικό της πιστοποιητικό. Για να κρατείται το πιστοποιητικό του

καταναλωτή στον προσωπικό του υπολογιστή ή κάρτα (Identification Card-IC), απαιτείται λογισμικό που καλείται **ηλεκτρονικό πορτοφόλι** ή *ψηφιακό πορτοφόλι.* Για να συνδεθεί το ψηφιακό πορτοφόλι με διάφορους εμπόρους, η διαλειτουργικότητα είναι ένα πολύ σημαντικό χαρακτηριστικό που πρέπει να ικανοποιείται.[3,5]



Πίνακας 5.4: Επισκόπηση των κύριων μηνυμάτων στο SET



Πίνακας 5.5: Οντότητες του πρωτοκόλλου SET στις κυβερνοαγορές

First Virtual

Η First Virtual (FV) (http://www.fv.com/) υλοποίησε και ανέπτυξε ένα από τα πρώτα ηλεκτρονικά συστήματα πληρωμών, το First Virtual Internet Payment System, τον Οκτώβριο του 1994. Όλως περιέργως, το FV δεν χρησιμοποιεί κρυπτογραφία ή ασφαλή μέσα επικοινωνίας. Αντίθετα μάλιστα, το σύστημα της πληρωμής βασίζεται στην ανταλλαγή e-mail μηνυμάτων και στην εντιμότητα των καταναλωτών. Το First Virtual παίζει το ρόλο του μεσολαβητή στις συναλλαγές πιστωτικών καρτών μεταξύ καταναλωτών και εμπόρων. Ένας καταναλωτής πρέπει πρώτα να εγκαταστήσει έναν λογαριασμό με FV. Ο λογαριασμός ασφαλίζεται με πιστωτικές κάρτες Visa ή MasterCard. Μετά την υπογραφή με FV, παρέχεται ο καταναλωτής με ένα ψηφιακό κωδικό πρόσβασης(Virtual PIN). Το Virtual PIN παίζει το ρόλο του πληρεξούσιο για το νούμερο της πιστωτικής κάρτας, το οποίο κρατιέται από την FV. Ένα ετήσιο ποσό 2$ χρεώνεται στους καταναλωτές με πιστωτική κάρτα.

Τα πλεονεκτήματα της First Virtual και τα οποία παρέχουν ασφάλεια ενάντια σε απάτες βασίζονται σε τρεις επιχειρηματικές πρακτικές:

- Τα νούμερα της πιστωτικής κάρτας δεν μεταφέρονται ποτέ μέσω Internet
- Επανειλλημένες επιθέσεις δεν είναι πιθανές
- Ένα έμπορος που είναι απλήρωτος για online παράδοση πληροφοριών για αγαθά παθαίνει αμελητέες ζημιές.

Παρ' όλα αυτά αν ένας πελάτης που έχει δώσει την ηλεκτρονική του διεύθυνση δεν ζητήσει να αποκλειστεί(excluded) η αθετημένη(default) αξία θα ξαναεπανέλθει για επανάληψη πληρωμής.[1]

Digicash

Στην Digicash (Chaum 1985), οι καταναλωτές κρατάνε τη νομισματική αξία μέσα σε μία φόρμα ηλεκτρονικών εμβλημάτων(tokens). Καταναλωτές και έμποροι ανταλλάσσουν εμβλήματα(tokens) και αυτά τα εμβλήματα επιβεβαιώνονται από μία τράπεζα. Η τράπεζα επιβεβαιώνει ότι οι υπογραφές πάνω στα εμβλήματα(token) είναι έγκυρες και ότι αυτά τα εμβλήματα(token) δεν έχουν ήδη ξοδευτεί.

Η Digicash παρέχει μόνο ένα μηχανισμό για ηλεκτρονική πληρωμή. Τα πρωτόκολλα της Digicash δεν παρέχουν μηχανισμούς για ανακάλυψη, διαπραγμάτευση, παράδοση ή ανάλυση σύγκρουσης(conflict resolution). Ο σκοπός της Digicash είναι μαζί η δύναμη και η αδυναμία της. Το πλεονέκτημά της είναι ότι παρέχει ένα κομψό και απλό πρωτόκολλο. Το μειονέκτημα της είναι ότι δεν μπορεί να προσφέρει μείωση τους κόστους που σχετίζεται με την συλλογή και αμφισβήτηση ανάλυσης.

Η Digicash είναι ένα υψηλά-ασφαλές σύστημα. Ο έμπορος που σε μια συναλλαγή χρησιμοποιεί Digicash έχει την απαραίτητη πληροφόρηση μόνο για να διασφαλίσει την πληρωμή ενώ η τράπεζα σε μια συναλλαγή έχει την απαραίτητη πληροφόρηση μόνο για να πιστώσει και να χρεώσει ένα λογαριασμό.[3]

6. ΑΣΦΑΛΕΙΑ ΔΙΑΚΟΜΙΣΤΗ

Ο διακομιστής που συνδέει την εταιρεία κάποιου με το Internet και το Internet με την εταιρεία είναι ένας σταθερός κίνδυνος. Είναι σημαντικό να έχει κάποιος μία σαφή ιδέα ποιοι είναι οι κίνδυνοι που περιβάλλουν τον διακομιστή και τι μέτρα ασφαλείας πρέπει να πάρει για να τον προστατεύσει. Ένα τέτοιο μέτρο είναι τα λεγόμενα φράγματα –**firewalls.**

FIREWALLS

Firewall (Φράγμα), είναι μια συσκευή υλικού ή λογισμικού, ένα σύστημα που επιβάλλει πολιτική ελέγχου πρόσβασης μεταξύ δύο δικτύων - όπως μεταξύ ενός ιδιωτικού τοπικού LAN και του επισφαλούς δημόσιου Διαδικτύου. Επίσης καθορίζει ποιες εσωτερικές υπηρεσίες μπορούν να προσεγγιστούν από το εξωτερικό περιβάλλον, και αντίστροφα. Τα μέσα με τα οποία αυτό ολοκληρώνεται ποικίλλουν ευρέως, αλλά σε γενικές γραμμές, το firewall μπορεί να θεωρηθεί ως ένα ζεύγος μηχανισμών: ένας για να εμποδίσει και ένας για να επιτρέψει την κυκλοφορία. Ένα firewall είναι κάτι περισσότερο από την κλειδωμένη μπροστινή πόρτα σε ένα σύστημα ή δίκτυο — είναι επίσης η φρουρά ασφάλειας του συστήματος.

Η έννοια του firewall είναι να παρέχει ένα ελεγχόμενα διαπερατό εμπόδιο μεταξύ του χρήστη PC και του Διαδικτύου κατά την διάρκεια της σύνδεσης. Το διαπερατό μέρος της υπόθεσης είναι σημαντικό, δεδομένου ότι ένα εμπόδιο που δεν θα επέτρεπε τίποτα να περάσει θα έκανε το σέρφινγκ στον Παγκόσμιο Ιστό αδύνατο. Εντούτοις, το εμπόδιο πρέπει να εφαρμόσει πολύ ακριβείς κανόνες για αυτό που επιτρέπεται και τι δεν είναι επιτρεπτό. Οι σελίδες από έναν επισκεπτόμενο κεντρικό υπολογιστή δικτύου είναι κάτι επιθυμητό να διαπεράσουν μέσω του firewall. Ένας κώδικας δούρειου ίππου όμως όχι!

Το firewall μπορεί να παρέχει σε έναν διαχειριστή δικτύων τα στοιχεία για τα είδη data και ποσό κυκλοφορίας που πέρασε μέσω αυτού, πόσες προσπάθειες έγιναν να σπάσουν το σύστημα ασφάλειας, και άλλες υπηρεσίες επίσης. Όπως ένα κλειστό σύστημα TV ασφάλειας κυκλωμάτων, το firewall όχι μόνο αποτρέπει την πρόσβαση, αλλά αποθαρρύνει και τους κακόβουλους ανιχνευτές του δικτύου που ανιχνεύουν τριγύρω για ανοικτές θύρες, και βοηθά επίσης στον προσδιορισμό εκείνων που προσπαθούν να παραβιάσουν την ασφάλεια ενός συστήματος. Το firewall αρχικά καθορίζει εάν η εισερχόμενη μετάδοση είναι κάτι που ζητείται από έναν χρήστη στο δίκτυο, και απορρίπτει όλα τα άλλα. Οτιδήποτε εισέρχεται εξετάζεται περισσότερο. Ελέγχεται η διεύθυνση υπολογιστών του πομπού για να εξασφαλιστεί ότι είναι εμπιστευμένη περιοχή ή όχι. Ελέγχεται επίσης το περιεχόμενο της μετάδοσης.

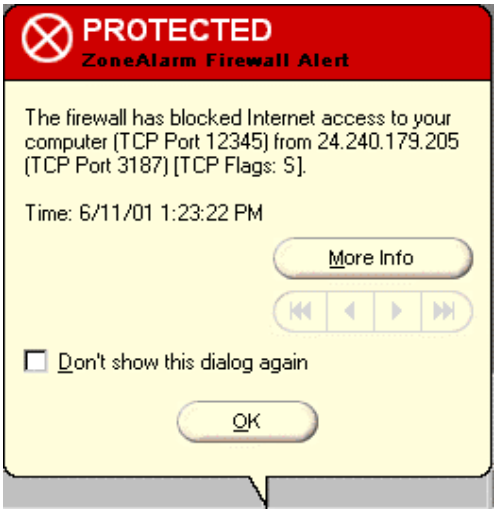
Εξ' αιτίας της θέσης τους στη τομή δύο δικτύων, μπορούν να εξυπηρετήσουν και άλλους σκοπούς, όπως να εμποδίσουν την πρόσβαση σε συγκεκριμένες τοποθεσίες του Διαδικτύου ή τη χρήση κάποιων εξυπηρετών ή υπηρεσιών. Ανάλογα με την μέθοδο διαλογής και αποτροπής πρόσβασης, είναι γνωστοί τρεις τύποι προϊόντων υλικού ή λογισμικού firewall:

- Απαγόρευση εισερχομένων δεδομένων τα οποία δεν έχουν ζητηθεί από τον χρήστη στο δίκτυο.
- Διαλογή από τη διεύθυνση του πομπού.
- Διαλογή από το περιεχόμενο της επικοινωνίας.

Ο οργανισμός ICSA τα ταξινομεί σε τρεις κατηγορίες: φίλτρων πακέτων, application-level proxy servers, και επιθεώρησης πακέτων.

Δημοφιλή Πακέτα Λογισμικού Personal Firewall

A) Zone Alarm™



Τα Zone Labs παρέχουν δωρεάν τη έκδοση Zone Alarm (download από το επίσημο Web Site). Το Zone Alarm λειτουργεί σε Stealth Mode, που καθιστά το PC κυριολεκτικά "αόρατο" στο διαδίκτυο. Το πρόγραμμα είναι κάτι παραπάνω από αρκετό για την προστασία ενός απλού χρήστη. Διαθέτει εξαιρετικά απλό interface και δίνει τη δυνατότητα στους χρήστες να αποφασίσουν ποια προγράμματα θα έχουν πρόσβαση στο Internet αλλά και να ορίσουν αν θα υπάρχει πρόσβαση κατά την απουσία τους. Τηρείται ημερολόγιο με τους συναγερμούς και συνεργάζεται και με προγράμματα ηλεκτρονικού ταχυδρομείου. Υπάρχει ακόμη πλήκτρο άμεσης διακοπής της σύνδεσης με το Internet.

Πλεονεκτήματα: Δωρεάν, προστασία από εξωτερικές επιθέσεις, εύκολο στην εγκατάσταση και στη χρησιμοποίηση.
Μειονεκτήματα: Ενοχλητική οθόνη στο ξεκίνημα.
Συμπέρασμα: Παρέχει-δωρεάν- εξαιρετική προστασία σε κάθε χρήστη που σερφάρει στο Ιντερνετ.

B) Norton Personal Firewall2002

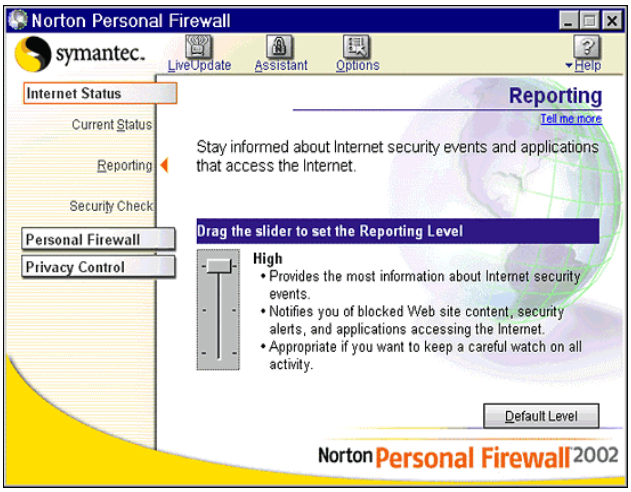
Το Norton Personal Firewall αποτελεί την πιο πρόσφατη έκδοση του προσωπικού πακέτου προστασίας της Symantec και περιλαμβάνει διάφορα καινοτόμα χαρακτηριστικά γνωρίσματα. Απαγορεύει προσωπικές και εμπιστευτικές πληροφορίες να στέλνονται σε μη ασφαλή Web Sites χωρίς την γνώση του χρήστη. Με την λειτουργία-δυνατότητα προστασίας εισβολών ειδοποιεί τον χρήστη όταν κάποιος χάκερ προσπαθεί να ανιχνεύσει τον υπολογιστή για ευπάθειες (τρωτότητα).

Για τους προηγμένους χρήστες, το προσωπικό firewall Norton προσφέρει έναν μακρύ κατάλογο προσαρμόσιμων κανόνων που ελέγχουν την πρόσβαση προς και από τον υπολογιστή με λεπτομέρειες ασφάλειας. Η εισερχόμενη ή εξερχόμενη επικοινωνία εμποδίζεται, εξ ορισμού, εκτός αν συγκεκριμένος κανόνας (rule) την επιτρέπει. Οι κανόνες ενεργοποιούνται αυτόματα όποτε συμβαίνει κάποιο "alert" και ο χρήστης αποφασίζει αν η πρόσβαση πρέπει να αμφισβητηθεί ή να επιτραπεί σε ένα συγκεκριμένο πρόγραμμα. Οι χρήστες μπορούν επίσης να διαμορφώσουν τους κανόνες από την αρχή, ενώ το πρόγραμμα παρέχεται με ένα σύνολο προκαθορισμένων κανόνων για τα πιο κοινά προγράμματα Δούρειων Ίππων (Trojan)&η Horses). Για τους περισσότερους χρήστες - μη ενδιαφερόμενους -για τις λεπτομέρειες ασφάλειας, παρέχεται η δυνατότητα επιλογής ενός επιθυμητού (υψηλό, μέσο, χαμηλό) επίπεδου.

Το πρόγραμμα ελέγχει τα εισερχόμενα cookies και περιλαμβάνει μέθοδο ελέγχου εφαρμογών HTTP, όπως οι φυλλομετρητές, για μη διαβίβαση ορισμένων λέξεων μέσω του Διαδικτύου, χωρίς τη δικαιοδοσία του χρήστη. Για παράδειγμα μπορεί κάποιος να εισάγει το όνομα, τη διεύθυνση, και τον τηλεφωνικό του αριθμό για να εμποδίζει αυτές τις πληροφορίες από την υποβολή σε φόρμες του Διαδικτύου

και άλλα απευθείας σύνδεσης εργαλεία. Αυτή η προστασία δεν εξετάζει προγράμματα μη- HTTP, όπως το ηλεκτρονικό ταχυδρομείο.

Μερικοί υποστηρίζουν ότι το nterface δεν είναι τόσο εύχρηστο όσο σε μερικά άλλα προϊόντα αυτής της κατηγορίας. Το κόστος ανέρχεται σε($29.95). Η Symantec δεν προσφέρει έκδοση ελεύθερης δοκιμής.



Πλεονεκτήματα: σταθερή προστασία και διπλή ζώνη άμυνας ενάντια σε μη εξουσιοδοτημένες συνδέσεις μέσω διαδικτύου.
Μειονεκτήματα: δεν απομονώνει ή επιτρέπει πρόσβαση σε συγκεκριμένα sites.
Συμπέρασμα: Ακριβό ώστε να ανταγωνισθεί το δωρεάν Zone Alarm.

Με την υποστήριξη για τα Windows XP, το Norton Personal Firewall 2002 προσθέτει περισσότερο διαμορφώσιμο έλεγχο της σύνδεσης με το Διαδίκτυο και στους τρόπους άμυνας ενάντια στις απειλές των χάκερ. Η γενική εικόνα της διεπαφής είναι συγκρίσιμη με τον εξερευνητή Windows, με την πλευρά πλοήγησης στα αριστερά και το παράθυρο πληροφοριών στα δεξιά. Υπάρχουν τρία προκαθορισμένα επίπεδα ελέγχου πρόσβασης: Υψηλό, μέσο και χαμηλό τα οποία επιλέγονται με μια απλή ράβδο κύλισης. Για τους πιο πεπειραμένους χρήστες, μπορεί να επιλεχτεί ένα προσαρμοσμένο επίπεδο. Από εδώ, μπορεί να ρυθμιστεί το επίπεδο ασφάλειας των συστατικών Java και ActiveX.

Ένα πρακτικό χαρακτηριστικό γνώρισμα που έχει περιληφθεί είναι η προαιρετική δυνατότητα εξωτερικής ανίχνευσης κινδύνου ασφάλειας (Security Risk Scan Option). Με την επιλογή αυτή συνδέεται ο υπολογιστής του χρήστη με τον ιστοχώρο της Symantec, ο οποίος τρέχει έπειτα μια ανίχνευση στο σύστημα. Ελέγχεται το σύστημα ενάντια στις πιο κοινές απειλές των χάκερς και δίνεται αναφορά για τα αποτελέσματα. Με το Live Update Program, το λογισμικό του firewall ενημερώνεται με τα πιο πρόσφατα στοιχεία για τις απειλές στον ιστοχώρο της Symantec. Για το πρώτο έτος μετά την αγορά η δυνατότητα αυτή παρέχεται δωρεάν ενώ στη συνέχεια η συνδρομή ενός έτους κοστίζει $9.95.

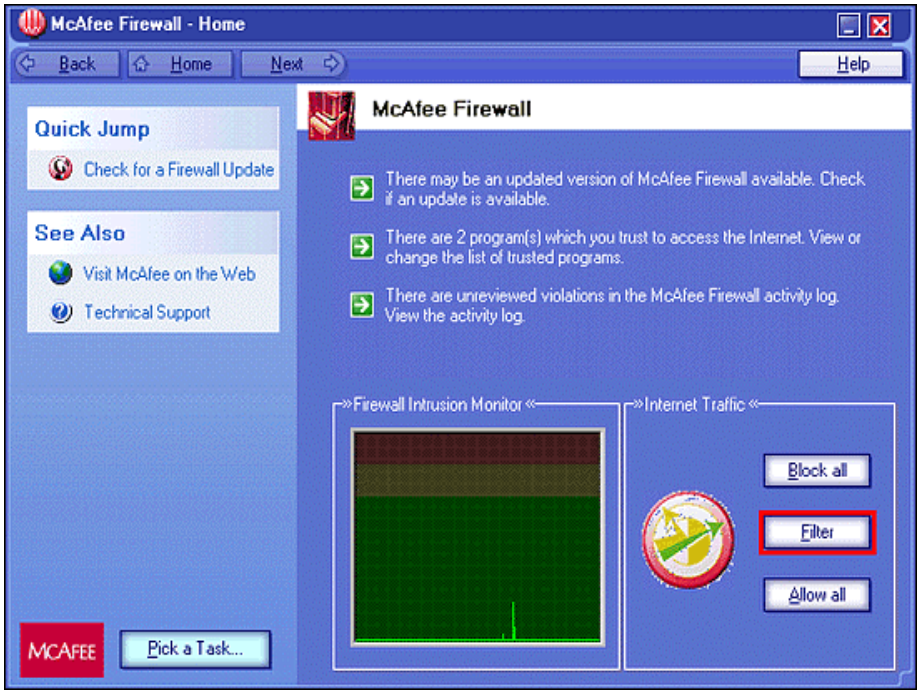
Γ) McAfee Personal Firewall

Το προσωπικό firewall McAfee.com είναι μια υπηρεσία απευθείας σύνδεσης που προσφέρει προστασία, μέσω ενός όχι και τόσο ισχυρού είναι αλήθεια interface, με χαρακτηριστικά γνωρίσματα διάφορους ήχους προειδοποίησης. Εν τούτοις, εκτελεί τα βασικά καθήκοντα. Εκτός από τη παρεχόμενη προστασία ενάντια στις εξωτερικές απειλές, το πρόγραμμα παρεμποδίζει άλλες εφαρμογές που προσπαθούν να πετύχουν πρόσβαση στο Διαδίκτυο.

Ενημερώνει τι συμβαίνει στον υπολογιστή σε καθημερινή ή εβδομαδιαία βάση. Καταγράφει την ενδεχομένως εχθρική κυκλοφορία στο Διαδίκτυο και προειδοποιεί με σαφείς δυνατότητες-επιλογές απάντησης για κάθε μια από τις σημειωθείσες προσπάθειες παρείσφρησης.

Το λογισμικό της εταιρίας McAfee πωλείται σε ετήσια βάση συνδρομής, ένα χαρακτηριστικό γνώρισμα που μπορεί να απευθυνθεί σε μερικούς, αλλά δεν υπάρχει έκδοση ελεύθερης δοκιμής. Η ετήσια τιμή συνδρομής εξουσιοδοτεί τους χρήστες στις

αυτόματες αναπροσαρμογές και βελτιώσεις. Οι αναπροσαρμογές προϊόντων εμφανίζονται "online" μέσω του Διαδικτύου. Επίσης το προσωπικό firewall McAfee.com μπορεί να χρησιμοποιηθεί από κοινού με άλλα προϊόντα McAfee. Παρέχει πλήρη, πολυεπίπεδη ασφάλεια σε PC όταν συνδυάζεται με πρόγραμμα VirusScan Online. Το κόστος του ανέρχεται περίπου στα 29.95$.[6]



Πλεονεκτήματα: Εύκολο στην εκμάθηση, παρουσιάζει την δραστηριότητα και υπάρχει στην κεντρική οθόνη ρύθμιση φίλτρων.
Μειονεκτήματα: Προσανατολισμένο σε XP
Συμπέρασμα: Χαμηλό κόστος με ικανοποιητική προστασία

Συγκρίσεις χαρακτηριστικών Personal Firewalls

Manufacturer	Zone Labs	Symantec	McAfee
Product:	Zone Alarm	Norton Personal Firewall	Firewall 3.0
FEATURES			
MD5 Signature Support	YES	NO	NO
Trusted Applications	YES	YES	YES
Trusted Address Groups	YES	YES	YES
Intrusion Detection	YES	YES	YES
Remote Administration	NO	NO	NO
Time Intervals	NO	NO	NO
Login Authentication	YES	NO	YES
Runs as Service	YES	YES	YES
File Size (Before Installation)	1,920 KB	43,377 KB	7,650 KB
Supported Operating Systems	95, 98, NT, 2k, ME	95, 98, NT, 2K	95, 98, NT
Prices	Free*	$ 29.95	$ 39.95

Product	Incoming protection	Outgoing protection	E-mail protection	Blocks specific IP addresses	Security logs
ZoneAlarm 2.6	Yes	Yes	Yes	No	Yes
Norton Personal Firewall 2002	Yes	Yes	No	No	Yes
McAfee Firewall 3.0	Yes	Yes	No	Yes	Yes

7. ΑΣΦΑΛΕΙΑ ΒΑΣΙΣΜΕΝΗ ΣΤΟ ΧΡΗΣΤΗ

Η ασφάλεια βασισμένη στο χρήστη αφορά εσωτερικά μέτρα ασφάλειας. Υπάρχουν δύο βασικά επίπεδα τέτοιας ασφάλειας:

- Το όνομα και ο κωδικός πρόσβασης του τελικού χρήστη, που όταν χρησιμοποιηθεί σωστά, δίνει στο χρήστη πρόσβαση στους διακομιστές της εταιρίας.
- Το όνομα και ο κωδικός πρόσβασης του διαχειριστή του δικτύου, που όταν χρησιμοποιηθούν μαζί σωστά, δίνουν δικαιώματα σε αυτό το διαχειριστή να έχει πρόσβαση σε συσκευές του δικτύου, για παρακολούθηση και συντήρηση.

Είναι δυνατόν εξωτερικοί χρήστες να έχουν πρόσβαση στο δίκτυο κάποιας εταιρείας, χρησιμοποιώντας διάφορες μεθόδους επίθεσης. Αν όμως αποτύχει μία ασφάλεια επιπέδου κίνησης, ένας εισβολέας μπορεί να σταματήσει μέσα από την ασφάλεια την βασισμένη στο χρήστη. Αν ένας εισβολέας μπορεί να μπει μέσα στο δίκτυο της εταιρείας, αυτός ο εισβολέας δεν θα μπορέσει να ταξιδέψει ελευθέρα μέσα στο δίκτυο.

Με την ασφάλεια τη βασισμένη στο χρήστη, κάθε χρήστης προσδιορίζεται ξεχωριστά, πιστοποιείται και ελέγχεται. Η διαδικασία της ασφαλείας χρήστη, που συνδέει το όνομα χρήστη με τον κωδικό πρόσβασης και επιτρέπει σε ένα χρήστη πρόσβαση στο δίκτυο, ονομάζεται *έλεγχος ταυτότητας, εκχώρηση δικαιωμάτων και λογαριασμοί* (authentication, authorization, accounting - AAA).

Έλεγχος Ταυτότητας

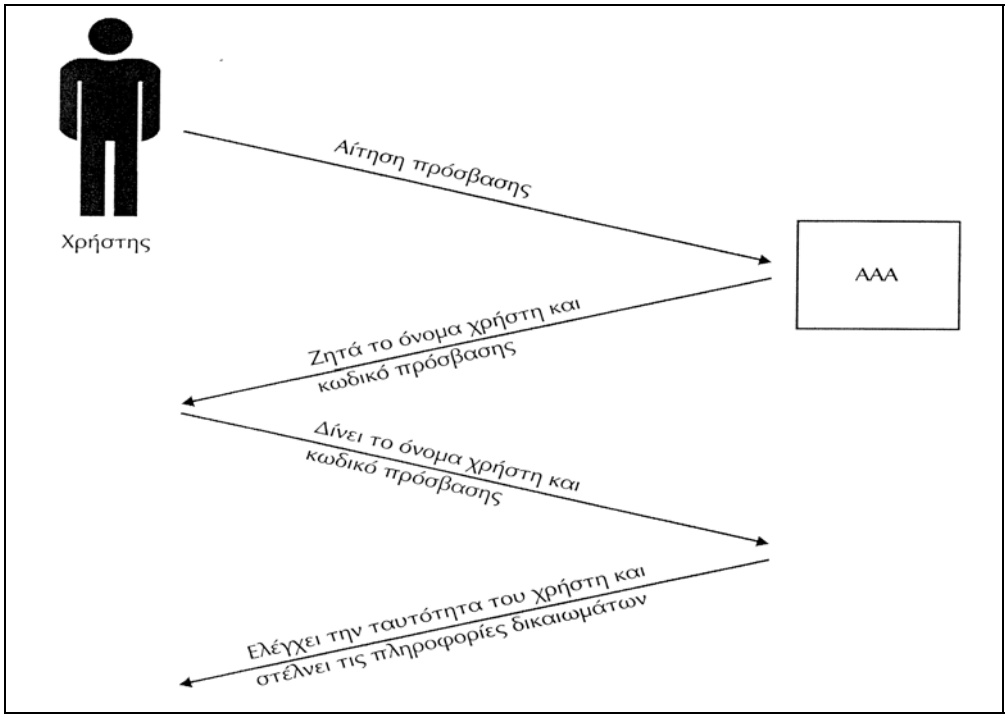
Ο *έλεγχος ταυτότητας* (authentication) είναι μία διαδικασία πιστοποίησης του χρήστη που ζητά πρόσβαση στο δίκτυο και αποφασίζει αν αυτός ο χρήστης θα πρέπει να έχει πρόσβαση. Κάθε χρήστης έχει μοναδικό όνομα χρήστη και κωδικό πρόσβασης.

Εκχώρηση Δικαιωμάτων

Η *εκχώρηση δικαιωμάτων* (authorization) είναι μία λίστα από άδειες που δίνονται σε ένα χρήστη για να έχει πρόσβαση σε μία συγκεκριμένη εφαρμογή του δικτύου. Επειδή αυτή κατανέμεται ως προς το όνομα χρήστη, δεν έχουν όλοι οι χρήστες την ίδια πρόσβαση σε όλες τις εφαρμογές.

Λογαριασμοί

Οι *λογαριασμοί* (accounting) είναι ένα τμήμα που διατηρεί εγγραφές για την ασφάλεια την βασισμένη στο χρήστη. Οι λογαριασμοί παρακολουθούν από πού είναι συνδεδεμένος ο κάθε ένας και για πόσο.



Η Λύση RADIUS

Υπάρχουν προγράμματα διαθέσιμα που κάνουν τη διαχείριση της ασφάλειας επιπέδου χρήστη πολύ ευκολότερη, ελέγχοντας τις πληροφορίες AAA σε μία βάση δεδομένων χρηστών που μπορεί να προσπελαστεί από διαφορετικούς διακομιστές και εφαρμογές. Ένα παράδειγμα τέτοιου πρωτοκόλλου είναι το RADIUS. Το RADIUS(Remote Authentication Dialing User Service), είναι ένα πρωτόκολλο ασφαλείας που επικεντρώνεται βασικά στην πιστοποίηση χρηστών και στη συντήρηση πληροφοριών γι' αυτούς.

Λειτουργία του RADIUS

Όταν ένας χρήστης προσπαθεί να συνδεθεί στο δίκτυο, ο πελάτης RADIUS ζητά το όνομα χρήστη και τον κωδικό πρόσβασης αυτού του χρήστη. Το πρώτο που κάνει ο διακομιστής RADIUS, είναι να βεβαιωθεί ότι ο πελάτης που ζητά την άδεια είναι έγκυρος. Αν ο πελάτης είναι εντάξει, η απόκριση στέλνεται μετά στο καθορισμένο RADIUS διακομιστή, όπου γίνεται αναζήτηση στη βάση δεδομένων για το αντίστοιχο ζευγάρι. Ο διακομιστής RADIUS αποφασίζει μετά αν θα αποδεχτεί, θα απορρίψει ή θα ζητήσει το όνομα χρήστη και κωδικό πρόσβασης. Αυτή τη στιγμή, το RADIUS μπορεί επίσης να επιλέξει να προκαλέσει το χρήστη για να βεβαιωθεί ότι είναι έγκυρος. Το RADIUS μπορεί να στείλει αυτή την πρόκληση με την μορφή κειμένου, στην οποία ο χρήστης πρέπει να απαντήσει με επιπλέον πληροφορίες. Αν το RADIUS αποφασίσει να δεχτεί το όνομα χρήστη και κωδικό πρόσβασης, στέλνει μία λίστα με εκχωρήσεις δικαιωμάτων συνδεδεμένων με αυτό το ζευγάρι, υπαγορεύοντας πού μπορεί να έχει πρόσβαση ο χρήστης. Καταγράφονται επίσης και από το RADIUS όλες οι πληροφορίες της σύνδεσης του χρήστη.

Το RADIUS χρησιμοποιεί UDP σαν πρωτόκολλο μεταφοράς και αυτό αποτελεί μία μεγάλη διαφορά μεταξύ του RADIUS και του πρωτοκόλλου TACACS+ που περιγράφεται μετά, που χρησιμοποιεί TCP.

Πλεονεκτήματα του RADIUS

Το RADIUS προφανώς εξοικονομεί χρόνο και χρήματα ελέγχοντας την ασφάλεια AAA σε ένα καθολικό επίπεδο. Κρυπτογραφεί επίσης, όλες τις πληροφορίες κωδικών πρόσβασης, κάνοντας πολύ δύσκολο για τους εισβολείς να λαμβάνουν και να διαβάζουν αυτές τις εμπιστευτικές πληροφορίες. Ένα άλλο βασικό

πλεονέκτημα είναι ότι ο πελάτης και ο διακομιστής RADIUS επικοινωνούν με τέτοιο τρόπο, που οι κρυπτογραφημένες πληροφορίες δεν στέλνονται ποτέ μέσω του δικτύου. Οι λειτουργίες λογαριασμών του RADIUS είναι επίσης εντυπωσιακές, γιατί μπορούν να χρησιμοποιηθούν ανεξάρτητα από τα θέματα ελέγχου ταυτότητας και εκχώρησης δικαιωμάτων, επειδή το RADIUS καταγράφει την αρχή και το τέλος κάθε σύνδεσης. Το RADIUS είναι το πιο χρησιμοποιούμενο πρωτόκολλο, επειδή είναι γρήγορο και καταλαμβάνει λιγότερη μνήμη από τα άλλα πρωτόκολλα.

Μειονεκτήματα του RADIUS

Το κύριο μειονέκτημα του RADIUS είναι τα πιθανά ανοίγματα που αφήνει στην ασφάλεια. Αν και το RADIUS κρυπτογραφεί τον κωδικό πρόσβασης, δεν κρυπτογραφεί το όνομα χρήστη, τις εκχωρήσεις δικαιωμάτων και τις πληροφορίες λογαριασμών. Ένας εισβολέας μπορεί να έχει πρόσβαση σε αυτές τις πληροφορίες και έτσι να φτάσει σε εμπιστευτικούς πόρους.

Η Λύση TACACS+

Όπως και το RADIUS, έτσι και το TACACS+ παρέχει τις υπηρεσίες ελέγχου ταυτότητας, εκχώρησης δικαιωμάτων και λογαριασμών σε ένα διακομιστή, που μπορεί να χειρίζεται όλη την ασφάλεια επιπέδου χρήστη. Το TACACS+ αναπτύχθηκε από το Cisco Systems και αναφέρεται σαν μία μορφή ασφαλείας βασισμένη στο χρήστη για πρόσβαση σε συσκευές διαδικτύου. (Ο όρος TACACS+ προέρχεται από το Terminal Access Controller Access Control System Plus)

Λειτουργία του TACACS+

Το TACACS+ λειτουργεί με ένα παρόμοιο τρόπο με το RADIUS. Το TACACS+ στέλνει το όνομα χρήστη και τον κωδικό πρόσβασης στην λίστα πρόσβασης του διακομιστή, που με τη σειρά της στέλνει τις πληροφορίες για τις εφαρμογές στις οποίες μπορεί να έχει πρόσβαση ο χρήστης. Το TACACS+ στέλνει ωστόσο, τις πληροφορίες για τον έλεγχο ταυτότητας, εκχώρησης δικαιωμάτων και λογαριασμών ξεχωριστά.

Το TACACS+ λειτουργεί σε επίπεδο πρωτοκόλλου TCP. Το βασικό πλεονέκτημα αυτού του επιπέδου πρωτοκόλλου είναι ότι βεβαιώνεται ότι έχει οριστεί μία σύνδεση και ότι λαμβάνονται οι πληροφορίες που στέλνονται.

Υπάρχουν πολλά πλεονεκτήματα στο TACACS+ . Για παράδειγμα, το TACACS+ επιτρέπει το ίδιο όνομα χρήστη και κωδικό πρόσβασης να δουλεύει σε πολλαπλά πρωτόκολλα, απλοποιώντας πολύ την ασφάλεια επιπέδου χρήστη για τα άτομα που χρησιμοποιούν το δίκτυο της εταιρείας κάθε μέρα. Οι χρήστες εξοικονομούν χρόνο σύνδεσης στο δίκτυο κάθε πρωί και ενοχλούνται λιγότερο γιατί δεν χρειάζεται να συνδεθούν σε κάθε εφαρμογή ξεχωριστά.

Το TACACS+ έχει πολύ δυνατές δυνατότητες ασφαλείας λογαριασμών. Το όνομα χρήστη, η διεύθυνση χρήστη, η υπηρεσία που προσπαθεί να χρησιμοποιήσει, το πρωτόκολλο που χρησιμοποιείται, οι ώρες που ξεκίνησε και σταμάτησε και η ημερομηνία, όλα αυτά καταγράφονται για κάθε σύνδεση.[4]

	Δημιουργός	Κρυπτογράφηση	Ταχύτητα	Διαχείριση ΑΑΑ	Πρωτόκολλο Μεταφοράς
RADIUS	Livingston Enterprises	Μόνο τον κωδικό πρόσβασης	Γρηγορότερο	Συνδυάζει εκχώρηση δικαιωμάτων και λογα-ριασμούς	UDP
TACACS+	Cisco	Ολόκληρο το πακέτο	Πιο αργό	Ξεχωρίζει τον έλεγχο ταυτότητας, την εκχώρηση δικαιωμάτων και τους λο-γαριασμούς	TPC

Πίνακας 7.1: Το TACACS+ και το RADIUS μαζί

8. ΑΣΦΑΛΕΙΑ ΣΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ(E-Mail)

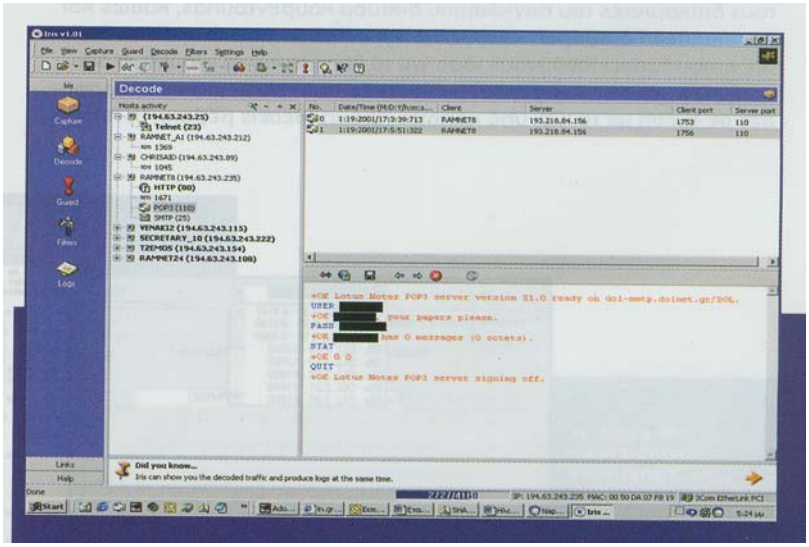
ΑΝ ΚΑΙ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ (E-MAIL) ΗΤΑΝ, είναι και, όπως όλα δείχνουν, θα συνεχίσει να είναι η δολοφονική εφαρμογή (killer application) του Διαδικτύου, ακόμα και σήμερα τα περισσότερα προγράμματα αποστολής και λήψης e-mail δεν εγγυώνται σε καμία περίπτωση τη διασφάλιση του προσωπικού απορρήτου του χρήστη ούτε και την ακεραιότητα της λειτουργίας του συστήματός του. Εξάλλου, ακόμα και ένας μέσος κράκερ γνωρίζει πολύ καλά ότι η υποκλοπή των ηλεκτρονικών μηνυμάτων υπό συγκεκριμένες συνθήκες είναι εξαιρετικά εύκολη υπόθεση. Για να κατανοήσει κάποιος το πώς είναι εφικτό κάτι τέτοιο, αξίζει να αναφερθούμε συνοπτικά στον τρόπο διακίνησης της ηλεκτρονικής αλληλογραφίας.

Κύριος φορέας των μηνυμάτων e-mail είναι το πρωτόκολλο επικοινωνίας SMTP (Simple Mail Transfer Protocol). Το SMTP αναλαμβάνει τη μεταφορά μηνυμάτων από το μηχάνημα του χρήστη σε ένα διακομιστή αλληλογραφίας (mail server), καθώς και την προώθηση του από έναν mail server σε κάποιον άλλο. Κάθε εταιρεία παροχής ιντερνετικών υπηρεσιών (Internet Provide Server) διαθέτει έναν ή περισσότερους διακομιστές αλληλογραφίας, οι οποίοι είναι υπεύθυνοι για την αποθήκευση και την αποστολή των μηνυμάτων. Όταν ένας χρήστης συνδέεται τηλεφωνικά (dialup) με τον ISP του, μπορεί να «κατεβάσει» την αλληλογραφία του από τον mail server του ISP στον υπολογιστή του, με τη βοήθεια του πρωτοκόλλου POP(Post Office Protocol) ή του IMAP(Internet Access Protocol)

Το ζήτημα της ασφάλειας που προκύπτει από τον τρόπο ανταλλαγής του e-mail, έγκειται στο γεγονός ότι τα πακέτα SMTP, τα οποία διέρχονται το δίκτυο του ιντερνετικού φορέα ή ένα εταιρικό δίκτυο, είναι δυνάμει προσπελάσιμα από οποιονδήποτε έχει πρόσβαση στο εκάστοτε δίκτυο και χρησιμοποιεί ένα εργαλείο ανάλυσης δικτύων (network diagnostics tool ή αλλιώς sniffer). Εργαλεία του είδους είναι διαθέσιμα στο Διαδίκτυο και μάλιστα οποιοσδήποτε μπορεί να τα βρει σχετικά εύκολα (ενδεικτικά παραθέτετε ο δικτυακός τόπος http://www.hideaway.net/Server_Security/Software/Sniffers/sniffers.html). Βασική λειτουργία των sniffer είναι η σύλληψη των πακέτων που διέρχονται έναν κόμβο ενός

οποιουδήποτε δικτύου. Ένας υπέρ το δέον αδιάκριτος χρήστης μπορεί να επιδοθεί στο «ευγενές» άθλημα της υποκλοπής ηλεκτρονικής αλληλογραφίας, κοινώς e-mail snooping, χρησιμοποιώντας ένα πρόγραμμα για «sniffing».

Ένας εκπρόσωπος της κατηγορίας των sniffer είναι το πρόγραμμα Iris της εταιρείας eEye Digital Security, για την πλατφόρμα των Windows. Μια δοκιμαστική αλλά πλήρως λειτουργική έκδοση του προγράμματος μπορεί κανείς να προμηθευτεί από το δικτυακό τόπο της εταιρείας (http://www.eeye.com/html). Το πρόγραμμα είναι ικανό να συλλαμβάνει όλα τα πακέτα δεδομένων τα οποία περνούν μια δεδομένη στιγμή από το τμήμα του δικτύου στο οποίο είναι συνδεδεμένος ο υπολογιστής που το φιλοξενεί.

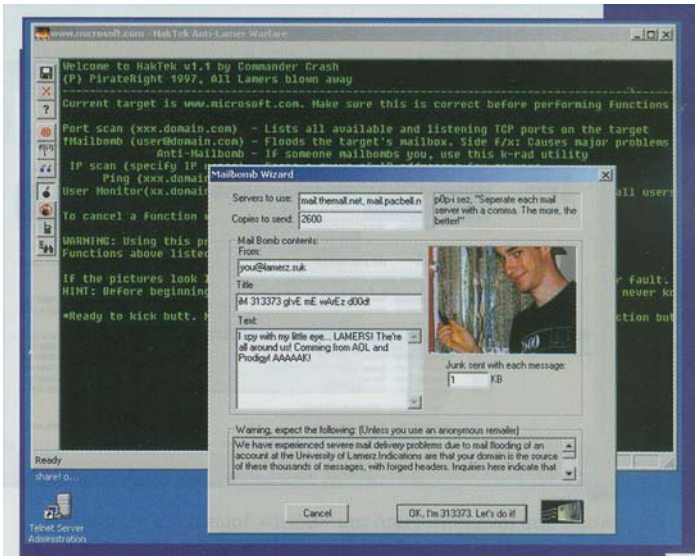


Εικόνα 8.1: Το πρόγραμμα Iris εν δράσει. Διακρίνονται τα πακέτα POP που απεστάλησαν όταν επιχειρήθηκε το «κατέβασμα» των e-mail από το διακομιστή αλληλογραφίας. Εκτός από το περιεχόμενο των e-mail που ελήφθησαν, τα περιεχόμενα των πακέτων POP αποκαλύπτουν τον κωδικό πρόσβασης(password), καθώς και το όνομα χρήστη(username), που χρησιμοποιούνται για την πρόσβαση στον εν λόγω διακομιστή.

Δυστυχώς, η υποκλοπή δεδομένων μέσω sniffer δεν αποτελεί το μόνο κίνδυνο για την αποστολή και τη λήψη ηλεκτρονικού ταχυδρομείου. Μια ιδιαίτερα προσφιλής πρακτική για όλους τους χαιρέκακους θαμώνες του Διαδικτύου είναι το λεγόμενο e-mail bombing. Η λογική του εν λόγω «βομβαρδισμού» είναι εξαιρετικά απλή και συνίσταται στην αποστολή μεγάλου αριθμού e-mail στο λογαριασμό ενός χρήστη; Οι περισσότεροι από εμάς θα έχουν παρατηρήσει πόσο χρονοβόρο και επίπονο είναι το κατέβασμα ενός e-mail, το μέγεθος του οποίου υπερβαίνει τα 3 ή 4MB, ιδιαίτερα στις αργές συνδέσεις dialup.

Εύκολα, λοιπόν, μπορεί κάποιος να φανταστεί τι θα συμβεί στην περίπτωση που κάποιος μας έχει αποστείλει μηνύματα e-mail, το συνολικό μέγεθος των οποίων είναι γύρω στα 50,100 ή και 500MB(!). Ο λογαριασμός του χρήστη καθίσταται ουσιαστικά άχρηστος αφού, προκειμένου να κατεβάσει το ηλεκτρονικό του ταχυδρομείο, οφείλει να κατεβάσει και ολόκληρα Mmegabyte «σκουπιδιών», που του έχει αποστείλει ο ανώνυμος «βομβιστής». Συνήθως, ο υπαίτιος του βομβαρδισμού φροντίζει να καλύπτει τα ίχνη του, εξαπολύοντας την επίθεση του από έναν κλεμμένο λογαριασμό ή μεταμφιέζοντας την ηλεκτρονική του διεύθυνση (IP spoofing).

Αν και οι επιθέσεις γίνονται συνήθως με χρήση ειδικών προγραμμάτων - σεναρίων (scripts), υπάρχει ένα πλήθος εξαιρετικά εύχρηστων προγραμμάτων στο Διαδίκτυο, τα οποία επιτρέπουν ακόμα και σε αδαείς να πραγματοποιούν... βομβαρδισμούς. Ένα από αυτά είναι το Hacktek (Εικόνα 8.2).



Εικόνα 8.2: Το πρόγραμμα Hacktek παρέχει τη δυνατότητα πραγματοποίησης επιθέσεων "mail bombing", αποκρύπτοντας ταυτόχρονα την πηγή της επίθεσης. Ο συγγραφέας του προγράμματος δεν δίστασε να ενσωματώσει και μια δική του φωτογραφία.

Μετά το mail bombing έρχεται ένα άλλο «ing», το spamming. Αν και δεν είναι καταστροφικό σαν το πρώτο, είναι σίγουρα άκρως εκνευριστικό. Ο όρος spamming αποδίδεται στην αυθαδέστατη τακτική που ακολουθούν πολλοί ιντερνετικοί τόποι, οι οποίοι ενοχλούν κατ' εξακολούθηση τους χρήστες με κάθε λογής διαφημιστικά μηνύματα και προσφορές, χωρίς προηγουμένως να έχουν λάβει την έγκριση τους. Οι ενοχλητικοί διαφημιστές συνήθως χρησιμοποιούν προγράμματα αυτόματης αναζήτησης ηλεκτρονικών διευθύνσεων (spambots), για να ανασύρουν ηλεκτρονικές διευθύνσεις από διάφορους δικτυακούς τόπους.

ΜΕΤΡΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ

Αν και οι κίνδυνοι από όλες τις προαναφερθείσες «μάστιγες» είναι όντως υπαρκτοί, σε καμία περίπτωση δεν είναι αναπόφευκτοι, αρκεί να λαμβάνονται ορισμένα απλά —ακόμη και στοιχειώδη-μέτρα προστασίας.

- **Κρυπτογράφηση e-mail**

Πολλά είναι τα προγράμματα αποστολής ηλεκτρονικού ταχυδρομείου, τα οποία υποστηρίζουν κάποια μορφή κρυπτογράφησης δεδομένων. Τα πακέτα που αποστέλλονται κρυπτογραφημένα είναι πρακτικά άχρηστα για τους χρήστες των sniffer, αφού ακόμα και μετά τη «συναρμολόγηση» τους δεν προκύπτει νόημα από τη μορφή τους. Η καλύτερη λύση για την κρυπτογράφηση μηνυμάτων , καθώς και αρχείων οιασδήποτε μορφής, προσφέρεται από το γνωστό, δωρεάν προσφερόμενο και πανίσχυρο σύστημα κρυπτογράφησης, το PGP (Pretty Good Privacy).

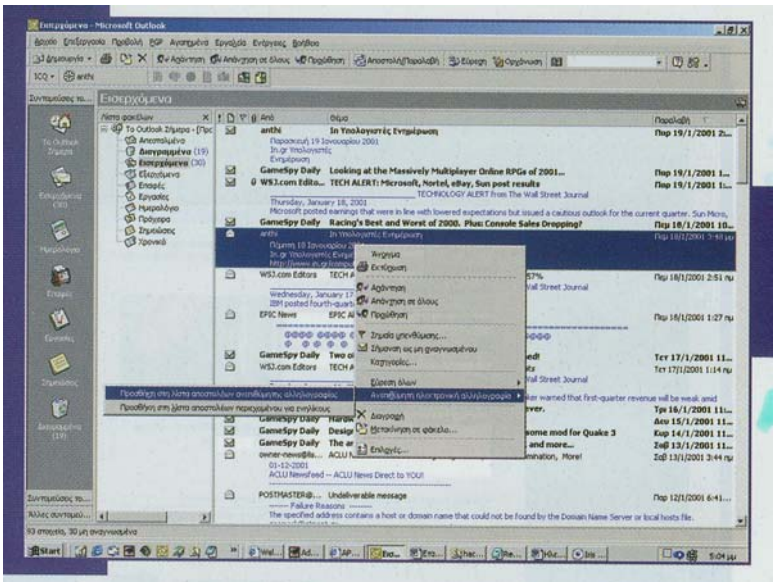
- **Αντιμετώπιση του spamming**

Συνήθως, ο παραλήπτης spam από ένα συγκεκριμένο δικτυακό τόπο, έχει τη δυνατότητα να διαγραφεί από μια σχετική λίστα παραληπτών, αρκεί να στείλει ένα e-mail με συγκεκριμένη μορφή σε κάποια ηλεκτρονική διεύθυνση που αναγράφεται στο τέλος του spam-mail (π.χ., ίσως πρέπει να στείλει ένα e-mail με τη λέξη «Unsubscribe» στη θυρίδα του θέματος -Subject). Στην περίπτωση, όμως, που δεν προσφέρεται η συγκεκριμένη δυνατότητα, τότε 9 χρήστης μπορεί να καταφύγει στις δυνατότητες φιλτραρίσματος του προγράμματος ηλεκτρονικής αλληλογραφίας που χρησιμοποιεί. Ο χρήστης του Outlook, για παράδειγμα, θα κάνει δεξί «κλικ» επάνω

στο ανεπιθύμητο e-mail, θα επιλέξει «Ανεπιθύμητη ηλεκτρονική αλληλογραφία» και θα προσθέσει τη διεύθυνση του αποστολέα στη λίστα των ανεπιθύμητων (Εικόνα 8.3). Επίσης, υπάρχουν δικτυακοί τόποι στους οποίους ο χρήστης μπορεί να απευθυνθεί για τη δίωξη των υπαιτίων ενοχλητικών μηνυμάτων (π.χ., http://www.cause.org-coalition against unsolicited commercial email/).

- **Αναζητώντας καταφύγια**

Η αντιμετώπιση του e-mail bombing είναι μια υπόθεση, η οποία (πρέπει να) απασχολεί πρώτιστα τους διαχειριστές κάθε ιντερνετικού φορέα και όχι τον ίδιο το χρήστη. Οι μεγαλύτεροι ISP μπορούν να εφοδιάσουν τους διακομιστές αλληλογραφίας με λογισμικό αυτόματης αντιμετώπισης τέτοιου είδους επιθέσεων όπως π.χ. το e-Safe Gateway της εταιρείας Alladin (http://www.ealaddin.com/esafe/gateway/index.asp)[2,8]



Εικόνα 8.3: Ο χρήστης του Outlook μπορεί να απαλλαγεί μια για πάντα από τα ανεπιθύμητα μηνύματα, προσθέτοντάς τα στη λίστα αποστολέων ανεπιθύμητης αλληλογραφίας του προγράμματος.

9. ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΙΟΥΣ

Η προστασία των σελίδων είναι ένας άλλος σημαντικός συντελεστής κίνδυνου, που όλες οι εταιρείες πρέπει να σκεφτούν όταν συνδέονται στο Internet. Στο παρελθόν, οι ιοί ήταν περιορισμένοι να μετακινούνται σε δίσκους. Συνήθως, οι χρήστες λάμβαναν μία δισκέτα από μία άλλη εταιρεία ή από μία αναξιόπιστη πηγή, η οποία μπορούσε να περιέχει έναν ιό. Αυτός ο ιός θα μπορούσε να βλάψει τους προσωπικούς υπολογιστές τους και μετά να μετακινηθεί στο δίκτυο. Αυτόν τον καιρό, οι ιοί έχουν διαδοθεί εξαιτίας του Internet.

Είναι σημαντικό να γνωρίζει κάποιος χρήστης για τους ιούς και για το πώς μπορούν να επηρεάσουν το δίκτυο του. Όχι μόνο μπορεί μία προγραμματισμένη απειλή να χαλάσει το ίδιο το δίκτυο κάποιου χρήστη, αλλά μπορεί να ανοίξει τις πόρτες και σε πολλούς άλλους εισβολείς. Κανένα μέτρο ασφαλείας δεν μπορεί να αντιμετωπίσει τις ανοικτές πόρτες που έχουν δημιουργηθεί από ειδικές, προγραμματισμένες απειλές. Όπως και οποιαδήποτε άλλη απειλή ασφαλείας, η καλύτερη προστασία είναι να μάθετε τις πιθανές επιθέσεις και να έχετε ένα πλάνο ενεργειών για να αντιμετωπίσετε τις πιθανές απειλές.

- Ένας *ιός (virus)* είναι ένα τμήμα κώδικα που δεν παραμένει στον εαυτό του, αλλά μπορεί να προσκολληθεί σε ένα άλλο πρόγραμμα και μετά να αναπαραχθεί μέσα σε

αυτό το πρόγραμμα. Οι ιοί μπορούν να έχουν διαφορετικά αποτελέσματα σε ένα δίκτυο. Μερικοί ιοί καταλαμβάνουν το πρόγραμμα και το κάνουν μη διαθέσιμο στους χρήστες. Άλλοι ιοί χαλούν κάποιο μέρος του προγράμματος, κάνοντας το πρόγραμμα να λειτουργεί λάθος. Τέλος, οι ιοί δουλεύουν επίσης επιβραδύνοντας το σύστημα, ώστε η απόδοση να είναι απαράδεκτη. Μπορούν να καταλάβουν πόρους και να περιορίσουν την πρόσβαση σε χρήστες που κανονικά μπορούν να έχουν πρόσβαση σε εφαρμογές και μερικές φορές οι ιοί μπορούν να χαλάσουν και δεδομένα.

- Ένα *worm (σκουλήκι)* είναι ένα πλήρες και ανεξάρτητο πρόγραμμα και από μόνο του αντιγράφει τον εαυτό του και διαδίδεται μέσω δικτύου. Όπως και ένας ιός, έτσι και το worm μπορεί να προκαλέσει προβλήματα σε δεδομένα, αλλά είναι πιο επικίνδυνο εξ αιτίας της δυνατότητας του να καταλαμβάνει ένα δίκτυο, να περιορίζει τους πόρους του ή ακόμα και να κλείνει ένα ολόκληρο δίκτυο.
- Ένα *Trojan Horse (Δούρειος Ίππος)* είναι μία εφαρμογή που δείχνει ότι είναι χρήσιμη και ασφαλής, αλλά έχει ένα άλλο πρόγραμμα μέσα σε αυτήν που μπορεί να χαλάσει το PC ή το δίκτυο. Το Trojan Horse είναι σαν ένα worm, αλλά είναι ένα ανεξάρτητο πρόγραμμα. Μπορεί να έχει τα ίδια αποτελέσματα όπως και ένα worm.

ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ

Τα εργαλεία προστασίας εναντίον των ιών είναι η καλύτερη προστασία εναντίον αυτών των προγραμμάτων. Αυτά τα αντιβιοτικά προγράμματα μπορούν να αγοραστούν online και εκτός σύνδεσης και να εγκατασταθούν κατευθείαν σε PC ή διακομιστές. Τα προγράμματα προστασίας ιών σαρώνουν το σύστημα σας ψάχνοντας και μετά καταστρέφοντας, προγραμματισμένες απειλές πριν δημιουργήσουν πρόβλημα. Είναι σημαντικό να διατηρείτε ενημερωμένα τα αντιβιοτικά σας προγράμματα, επειδή δημιουργούνται νέες απειλές κάθε μέρα. Η καλύτερη πολιτική είναι να ψάχνετε το Internet συχνά για πληροφορίες και αντιβιοτικά. Ο Πίνακας 9.1 δείχνει μερικές γρήγορες συμβουλές για την προστασία του δικτύου σας από ιούς.

Συμβουλές	Αιτία
Ψάχνετε το Internet συχνά για να βρείτε νέες ενημερώσεις ιών	Εμφανίζονται νέες πληροφορίες καθημερινά. Η ασφάλεια δικτύων έχει συνεχώς προβλήματα και μετά βελτιώνεται.
Τρέξτε το αντιβιοτικό πρόγραμμα ανίχνευσης εκτός σύνδεσης	Αν ένας ιός μπει στο δίκτυό σας, μπορεί να χαλάσει το αντιβιοτικό σας πρόγραμμα τόσο εύκολα, όπως οποιαδήποτε άλλη εφαρμογή. Ένα πρόγραμμα που τρέχει εκτός σύνδεσης είναι η καλύτερη προστασία σας.
Εκπαιδεύστε τους χρήστες για να προσδιορίζουν πιθανές, προγραμματισμένες απειλές	Οι ιοί συνήθως μπαίνουν στα δίκτυα μέσα από PC χρηστών. Για παράδειγμα, οι χρήστες ανοίγουν προγράμματα ή έγγραφα από μολυσμένες δισκέτες, ανοίγουν χαλασμένα μηνύματα ηλεκτρονικού ταχυδρομείου ή μεταφέρουν προγράμματα από το Internet που εκθέτουν το δίκτυο σε ιούς.
Μεταφέρετε νέα αντιβιοτικά, προγράμματα όταν γίνονται διαθέσιμα	Επειδή οι ιοί αλλάζουν κάθε φορά που συναντούνται νέοι ιοί, είναι σημαντικό να διατηρείτε το πρόγραμμά σας ενημερωμένο όσο γίνεται.

Πίνακας 9.1: Γρήγορες συμβουλές για ιούς

Τα αντιβιοτικά προγράμματα είναι ένα σημαντικό μέρος για να προλαβαίνετε τους ιούς. Υπάρχουν πολλά αντιβιοτικά προγράμματα και πολλές διαφορετικές επιλογές. Η καλύτερη ιδέα είναι να πάρετε ένα αντιβιοτικό πρόγραμμα που ψάχνει για πολλά διαφορετικά σημάδια. Όταν επιλέγετε ένα προμηθευτή, να θυμάστε ότι

πρέπει να έχετε ένα πρόγραμμα που να αναβαθμίζεται εύκολα, αφού οι ιοί αλλάζουν συνεχώς. Ένας προμηθευτής θα πρέπει να σας εξηγεί τις διαφορετικές αναβαθμίσεις, να είναι οι αναβαθμίσεις εύκολα προσπελάσιμες και να είναι μία αξιόπιστη εταιρεία. Για παράδειγμα, δεν θα θέλατε να ξοδέψετε πολύ χρόνο και χρήματα εγκαθιστώντας αντιβιοτικά προγράμματα, αν μία εταιρεία θα σταματήσει να δουλεύει και δεν θα έχετε πλέον ενημερώσεις. Ο Πίνακας 9.2 δείχνει μερικές εταιρείες αντιβιοτικών προγραμμάτων και τις Web διευθύνσεις τους.[4]

Εταιρεία Αντιβιοτικού Προγράμματος	Web Διεύθυνση
SecureNet Technologies	www.securenet.org
SafetyNet	www.safetynet.com/default.asp
Network Associates (McAfee)	www.nai.com
Cybersoft, Inc	www.cyber.com
ChekWARE	www.chekware.com
Central Command	www.avp.com
Alwil Software	www.alwil.com/en/default.asp

Πίνακας 9.2: Διευθύνσεις Αντιβιοτικών Προγραμμάτων

10. ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ ΚΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Οι έμποροι προκειμένου να μετρήσουν τις καταναλωτικές προτιμήσεις του κοινού με σκοπό να προσαρμόσουν στη βάση ζήτησης τις γραμμές παραγωγής τους και να προωθήσουν τις πωλήσεις τους μέσω του διαδικτύου, δημιουργούν νέους τρόπους συλλογής, επεξεργασίας και διασύνδεσης των προσωπικών δεδομένων. Τα προσωπικά δεδομένα συνήθως συλλέγονται κατά την αρχική φάση σύνδεσης του πελάτη με το δικτυακό χώρο του πωλητή και στην συνέχεια χρησιμοποιούνται σύγχρονες τεχνικές εξόρυξης δεδομένων (data mining) για την περαιτέρω ανάλυση τους. Αποτέλεσμα της παραπάνω διαδικασίας είναι η δημιουργία βάσεων καταναλωτικών προφίλ των πελατών. Προφίλ ενός ατόμου νοείται ως μια συλλογή δεδομένων που μπορεί μοναδικά να προσδιορίσει την ταυτότητα του ατόμου αυτού.

Οι οντότητες οι οποίες τυπικά εμπλέκονται στην εγκατάσταση μιας ηλεκτρονικής σύνδεσης, με έμφαση στων πραγματοποίηση ηλεκτρονικών συναλλαγών και οι οποίες είναι ταυτόχρονα η πηγή και ο αποδέκτης των προσωπικών δεδομένων των χρηστών είναι οι εξής:

1. Χρήστης

Ο ενδιαφερόμενος για την απόκτηση μιας υπηρεσίας του διαδικτύου, την απόκτηση ενός προϊόντος με χρήση τεχνολογιών που βοηθούν στην ανάπτυξη του ηλεκτρονικού εμπορίου κ.λ.π.

2. Παροχέας Υπηρεσιών Διαδικτύου, ΠΥΔ, (Internet Service Provider, ISP):

Η οντότητα που παρέχει, τυπικά σε χρήστες, το υλικό (hardware) και πιθανώς λογισμικό (software), για την απόκτηση πρόσβασης στις βασικές υπηρεσίες του διαδικτύου.

3. Παροχέας Φυσικού Μέσου επικοινωνίας, ΠΦΜ, (Carrier Provider):

Η οντότητα που παρέχει το φυσικό τεχνολογικό μέσο μετάδοσης και επικοινωνίας δεδομένων π.χ. αναλογικές ή και ψηφιακές γραμμές, εξοπλισμός αναμετάδοσης σημάτων με χρήση ψηφιακών κέντρων, δορυφόρων κ.λ.π. Οι οντότητες αυτές τυπικά αντιπροσωπεύονται από μεγάλους τηλεπικοινωνιακούς οργανισμούς π.χ. ΟΤΕ.

4. Παροχέας Τελικής Υπηρεσίας ΠΤΥ

Η οντότητα που παρέχει με χρήση κάποιου πρωτοκόλλου επικοινωνίας, την ζητούμενη από τον χρήστη υπηρεσία π.χ. αναζήτηση πληροφοριών με χρήση μηχανών αναζήτησης (search machines), αγορά προϊόντων με χρήση τεχνολογιών ανάπτυξης ηλεκτρονικού εμπορίου κ.λ.π.

Δύο επιπλέον οντότητες που παίζουν σημαντικό ρόλο στην διεκπεραίωση των ηλεκτρονικών συναλλαγών αλλά δεν εμπλέκονται, συνήθως, άμεσα σε αυτές είναι:

1. Έμπιστες Τρίτες Οντότητες (ΕΤΟ)

Αυτές είναι έμπιστες οντότητες οι οποίες δεν εμπλέκονται άμεσα στην συναλλαγή αλλά μπορούν να καταφύγουν οι εμπλεκόμενοι μιας συναλλαγής σε περιπτώσεις διενέξεων, για την επαλήθευση των στοιχείων της συναλλαγής. Τυπικό έργο των οντοτήτων αυτών είναι η έκδοση και διαχείριση ψηφιακών πιστοποιητικών (digital certificates). Οι ΕΤΟ συναντούνται στην βιβλιογραφία και με τον όρο Αρχές Πιστοποίησης (ΑΠ).

2. Λοιποί ενδιάμεσοι

Αυτές είναι τυπικά οι Τράπεζες που εμπλέκονται στην εκκαθάριση των πληρωμών είτε αυτές πραγματοποιούνται με τεχνολογίες ψηφιακού χρήματος είτε με χρήση πιστωτικών καρτών.

Στην Ελλάδα το βασικό νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων, καθορίζεται από τους νόμους 2472/97 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) και 2774/99 (Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα) με τον οποίο η Αρχή Προστασίας Δεδομένων και η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων έχουν αντίστοιχες αρμοδιότητες όπως ο νόμος αυτός ορίζει. Κάθε συλλογή και επεξεργασία στοιχείων των χρηστών του διαδικτύου (π.χ. ηλεκτρονική διεύθυνση αλληλογραφίας, διεύθυνση διαδικτύου κ.λ.π) εμπίπτουν στις διατάξεις των παραπάνω νόμων. Οποιαδήποτε χρήση των τηλεπικοινωνιακών υπηρεσιών όπως ορίζονται στο νόμο 2774/99 προστατεύεται από τις ρυθμίσεις για το απόρρητο των επικοινωνιών. Η άρση του απορρήτου σε δημόσιες αρχές είναι επιτρεπτή μόνο για τους λόγους και υπό τους όρους και διαδικασίες που ορίζει ο Ν. 2225/94 όπως ισχύει.

<u>Οι κίνδυνοι</u>

Ο χώρος του ηλεκτρονικού εμπορίου κρύβει πολλούς κινδύνους για τον ανυποψίαστο χρήστη. Οι περιπτώσεις όπου διακριτά καταγράφονται προσωπικά δεδομένα διακρίνονται στις παρακάτω κατηγορίες:

1. Όταν **με τη συγκατάθεση του** ο χρήστης δίνει τα προσωπικά του στοιχεία, όποτε για παράδειγμα επιθυμεί να αγοράσει κάποιο προϊόν / υπηρεσία ή να κατεβάσει *(download)* κάποιο πρόγραμμα στον προσωπικό του υπολογιστή ή και να εγγραφεί σε κάποια υπηρεσία του διαδικτύου. Προσωπικά δεδομένα, όπως στοιχεία ταυτότητας, στοιχεία επαγγελματικά, στοιχεία εκπαίδευσης η και ακόμα οικονομικά στοιχεία όπως είναι ο αριθμός της πιστωτικής κάρτας.

2. Όταν **χωρίς την συγκατάθεση του** χρήστη, συλλέγονται προσωπικά στοιχεία μέσω των λεγόμενων προγραμμάτων cookies τα οποία καταγράφουν και

επεξεργάζονται την συμπεριφορά του χρήστη κατά την πλοήγηση του στο διαδίκτυο (π.χ. προτιμήσεις).
3. Όταν στα πλαίσια του παροχέα υπηρεσιών πρόσβασης στο Internet τηρείται αρχείο με τα προσωπικά στοιχεία του χρήστη και κατ' επέκταση στοιχεία των ηλεκτρονικών διευθύνσεων (ιστοσελίδες) τις οποίες επισκέπτεται, τον ακριβή χρόνο και τη διάρκεια της επίσκεψης.

Ασφάλεια Προσωπικών Δεδομένων

Άλλο ένα θεμελιώδες θέμα ασφαλείας συνίσταται στη διαφύλαξη του προσωπικού απορρήτου, το οποίο πλέον αποτελεί ένα ακανθώδες ζήτημα στο Internet. Ένας μεγάλος όγκος πληροφοριών μπορεί να συλλεχθεί σχετικά με τους χρήστες του Δικτύου και πολλές φορές δεν είναι ξεκάθαρο ποιος ή με ποιο τρόπο θα χρησιμοποιήσει αυτές τις πληροφορίες. Συγκεκριμένα, δυο από τις σημαντικότερες τεχνολογίες που σχετίζονται με το θέμα είναι: **α)** τα cookies και **β)** το Web tracking.

Μέσω των Internet passports, διασφαλίζεται το προσωπικό απόρρητο του χρήστη, ενώ ταυτόχρονα επιτρέπεται στα Web sites να συλλέγουν πληροφορίες που χρειάζονται για να προσφέρουν εξειδικευμένες υπηρεσίες στους επισκέπτες τους. Η πιο κοινή χρήση των δεδομένων αυτών είναι η "διευκόλυνση" της εισόδου των χρηστών σε Web sites που ζητούν όνομα χρήστη και password.

Το cookie που βρίσκεται στο σκληρό δίσκο περιλαμβάνει το όνομα του χρήστη και το password, με αποτέλεσμα να μη χρειάζεται να δηλώνονται κάθε φορά, αφού τα στέλνει στον server και ο χρήστης εισέρχεται στο site ελεύθερα Τα cookies μπορεί να περιλαμβάνουν σχεδόν κάθε είδος πληροφοριών, όπως την τελευταία φορά που ένας χρήστης επισκέφθηκε κάποιο site, τα αγαπημένα του sites και άλλες παρόμοιες πληροφορίες. Μπορούν, επίσης, να χρησιμοποιηθούν για την παρακολούθηση των χρηστών όσο βρίσκονται σε κάποιο site και τη συλλογή πληροφοριών σχετικών με τις σελίδες που προτιμούν να επισκέπτονται.

Εκτός από τα cookies, υπάρχουν και άλλες μέθοδοι παρακολούθησης του τρόπου με τον οποίο οι χρήστες χρησιμοποιούν ένα Web site. Μία από αυτές προτείνει τη λεπτομερή εξέταση του ημερολογίου λειτουργίας του Web server. Η εξέταση αυτή επιτρέπει τον προσδιορισμό των δημοφιλέστερων σελίδων του site, των sites που μόλις επισκέφτηκαν οι χρήστες , του αριθμού των σελίδων που διαβάζουν σε μία τυπική επίσκεψη και άλλων σχετικών πληροφοριών.

Άλλες μέθοδοι στηρίζονται στη χρήση ορισμένων προγραμμάτων λογισμικού, στα sniffers τα οποία εξετάζουν κάθε πακέτο που εισέρχεται ή εξέρχεται από ένα Web site. Για τη διαφύλαξη του ιδιωτικού απορρήτου έχουν αναπτυχθεί αρκετές τεχνολογίες και πρότυπα. Σε αυτά περιλαμβάνονται τα Platform for Privacy Preferences (P3P),Internet Content and Exchange standard (ICE) και Open Profiling Standard (OPS). Οι τεχνολογίες αυτές ονομάζονται γενικά Internet passports. Τα Internet passports επιτρέπουν στους χρήστες να ελέγχουν ποιες προσωπικές πληροφορίες θα γίνουν διαθέσιμες στα Web sites, καθώς και τον τρόπο με τον οποίον αυτά θα τις χρησιμοποιήσουν. Επιτρέπουν, επίσης , στους χρήστες να ελέγχουν το είδος των πληροφοριών που θα συλλέξει το site κατά τη διάρκεια της πλοήγησης τους και το πώς θα τις χρησιμοποιήσει.[7]

11. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ (SECURITY POLICY)

Σκοπός της πολιτικής ασφάλειας πληροφοριών είναι η παροχή κατευθύνσεων και υποστήριξης για ζητήματα ασφάλειας πληροφοριών. Η διοίκηση του οργανισμού θα πρέπει να καθορίσει μια σαφή και ξεκάθαρη πολιτική, την οποία και θα υποστηρίζει έμπρακτα. Η πολιτική αυτή θα πρέπει να ρυθμίζει ζητήματα ασφάλειας σε όλα τα επίπεδα του οργανισμού.

Κείμενο της πολιτικής ασφαλείας

Το κείμενο της πολιτικής ασφάλειας θα πρέπει να γίνει αποδεκτό από τη διοίκηση του οργανισμού. Στη συνέχεια θα πρέπει να δημοσιοποιηθεί σε όλους τους υπαλλήλους. Θα πρέπει να αναφέρει τη δέσμευση της διοίκησης και τον τρόπο προσέγγισης του οργανισμού σε θέματα ασφάλειας. Θα πρέπει τουλάχιστον να περιλαμβάνει τα ακόλουθα:

- Τον ορισμό της ασφάλειας των πληροφοριών, το σκοπό της και τη σπουδαιότητα της ως μηχανισμού που επιτρέπει την ανταλλαγή πληροφοριών.
- Τους σκοπούς της διοίκησης και την υποστήριξη της αναφορικά με την ασφάλεια.
- Την επεξήγηση της πολιτικής ασφάλειας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιήσει ο οργανισμός, όπως σχετική νομοθεσία, προστασία από ιούς, επιπτώσεις μη συμμόρφωσης με την πολιτική ασφάλειας, διαχείριση επιχειρηματικής συνέχειας κ.λ.π.
- Τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας και την αναφορά συμβάντων.
- Αναφορές σε άλλα κείμενα που μπορούν να υποστηρίξουν την πολιτική ασφάλειας, όπως περιγραφές συγκεκριμένων διαδικασιών και κανονισμών.

Η πολιτική ασφαλείας θα πρέπει να κοινοποιείται σε ολόκληρο τον οργανισμό, έχοντας κατά περίπτωση την κατάλληλη μορφή.

Έλεγχος και αξιολόγηση

Θα πρέπει να υπάρχει ένας υπεύθυνος για την πολιτική ασφάλειας, καθήκον του οποίου θα είναι ο περιοδικός έλεγχος και η αναπροσαρμογή της μέσω προκαθορισμένων διαδικασιών. Οι διαδικασίες αυτές θα πρέπει να διασφαλίζουν ότι οποιεσδήποτε αλλαγές γίνονται αντικατοπτρίζουν μεταβολές που προκύπτουν από την αποτίμηση των κινδύνων που αντιμετωπίζει ο οργανισμός, όπως αλλαγές στη δομή του, ανακάλυψη νέων τρόπων επιθέσεων κλπ. Επίσης θα πρέπει να γίνεται περιοδικός έλεγχος σύμφωνα με τα ακόλουθα:

- Την αποτελεσματικότητα της πολιτικής σύμφωνα με καταγεγραμμένα περιστατικά ασφάλειας.
- Το κόστος των μηχανισμών προστασίας και τις επιπτώσεις τους στην λειτουργία του οργανισμού.
- Την εξέλιξη της τεχνολογίας.[9]

12. ΕΠΙΛΟΓΟΣ

Η ποσότητα της γνώσης γύρω από τα τεχνικά θέματα του διαδικτύου είναι σταθερή, ωστόσο το ίδιο το διαδίκτυο συνεχίζει να αυξάνει. Με άλλα λόγια, υπάρχουν πολλοί χρήστες του Internet με λίγη ή ακόμα και ανύπαρκτη γνώση για τους δυνητικούς κινδύνους που διατρέχουν, πόσο μάλλον για τα διαθέσιμα μέτρα προστασίας. Την ίδια στιγμή, το Internet βρίθει δικτυακών τόπων με εργαλεία και οδηγίες για «κράκινγκ» (cracking). Μάλιστα τα προγράμματα – εργαλεία είναι με τέτοιον τρόπο σχεδιασμένα, ώστε να μπορούν να χρησιμοποιηθούν ακόμα και από χρήστες με λιγοστές γνώσεις.

Στην πράξη, κανένας υπολογιστής online δεν μπορεί να είναι απόλυτα ασφαλής. Μολαταύτα, εάν κάποιος αναγνωρίσει την ύπαρξη των κινδύνων και αποφασίσει να προστατευτεί, μπορεί να είναι σε πολύ μεγάλο ποσοστό βέβαιος ότι δεν θα πέσει θύμα κανενός επιπόλαιου κράκερ(cracker). Αρκεί να χρησιμοποιήσουμε κατάλληλα προγράμματα προστασίας, όπως αυτά που παρουσιάστηκαν και να ακολουθήσουμε πιστά τους κανόνες που χαρακτηρίζουν τον σώφρονα κυβερνοπολίτη.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. **E-Commerce Security** - Anup K.Ghosh 1998
2. **RAM** Τεύχος 144 - σελίδες 100-128 - Φεβρουάριος 2001
3. **Trust And Risk Internet Commerce -** L. Jean Camp 2000
4. **Ε-επιχειρείν Πλήρης Οδηγός Ανάλυσης Τεχνικών Και Εμπορικών Θεμάτων** - Εκδότης Μ. Γκιούρδας 2001
5. **Ηλεκτρονικό Εμπόριο** - Turban, Lee, King, Chung 2002
6. **Firewalls** - Χρήστος Βένετης
http://www.conta.com.gr/conta/ekpaideysh/metaptyxiaka/e_commerce/ergasies/2002/Venetis/firewalls.pdf
7. **Ασφάλεια Στο Ηλεκτρονικό Εμπόριο** - Θρήσκου Χρυσάνθη-Μήλιου Αικατερίνη
http://www.conta.uom.gr/conta/ekpaideysh/metaptyxiaka/e_commerce/ergasies/2002/Thriskou/MBAecom.pdf
8. **Αντιμετώπιση των ανεπιθύμητων ηλεκτρονικών μηνυμάτων** – Δημήτρης Μπιμπίκας
http://www.conta.uom.gr/conta/ekpaideysh/metaptyxiaka/e_commerce/ergasies/Blocking_Mail.pdf
9. **Ασφάλεια πληροφοριακών και επικοινωνιακών συστημάτων στο χώρο του ηλεκτρονικού επιχειρείν**
http://forum.ebusiness.uoc.gr/