ΑΕΙ ΠΕΙΡΑΙΑ ΤΤ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Τεχνολογικό Εκπαιδευτικό Ίδρυμα
Τ.Ε.Ι. ΠΕΙΡΑΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια & Ιδιωτικότητα στο Διαδίκτυο

Security & Privacy on the Internet

Του Φοιτητή: Νικόλαος Γιανναράκης ΑΜ: 40360

Επιβλέπων Καθηγητής: Σταμάτης Αλατσαθιανός

Ιδιότητα: Καθηγητής

ΑΘΗΝΑ 2016

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εκπονήθηκε στα πλαίσια φοίτησης στο τμήμα Ηλεκτρονικών Υπολογιστικών συστημάτων του ΤΕΙ Πειραιά. Σκοπός της εργασίας είναι να αναδείξει και να αναφέρει πόσο σημαντική είναι η ασφάλεια στο διαδίκτυο και τι τρόποι προστασίας υπάρχουν. Στην εργασία αυτή γίνεται αναφορά στην ασφάλεια του εξυπηρετητή Web και τους τρόπους προστασίας που υπάρχουν. Αναφέρεται εκτενέστερα για τους ιούς και τα σκουλήκια καθώς και οι τρόποι αντιμετώπισής τους όπως τοίχοι προστασίας και άλλα λογισμικά προστασίας π.χ. τα antivirus. Άλλο ένα θέμα που θα αναφερθεί στην εργασία είναι ο λόγος που θέλουμε να υπάρχει εμπιστευτικότητα ανάμεσα σε δυο χρήστες όταν υπάρχει μεταφορά δεδομένων και πως η κρυπτογράφηση και τα είδη της συμβάλουν σε αυτό και πως χρησιμοποιούνται το δημόσιο και το ιδιωτικό κλειδί. Επίσης το ηλεκτρονικό εμπόριο το οποίο είναι πια ένα από τους δημοφιλέστερους τρόπους εμπορίου αντιμετωπίζει τα ίδια προβλήματα, καθώς πολλοί επιτήδειοι βρίσκουν διάφορους μεθόδους υποκλοπής για να υποκλέψουν πληροφορίες.

ABSTRACT

This project was worked out studies within the department of Electronic Computer Systems of TEI Piraeus. The purpose of this paper is to highlight and indicate how important online security is and what methods of protection are available. In this paper refers to the security of the Web server and what protection methods extensively exists. Refers for viruses and worms as well as ways of dealing with them such as firewalls and other software's protection, for example antivirus. Another issue that will be reported to work is why we want to have confidentiality between two users when data is being transferred and that of encryption and the already contribute to it and how the public key and private key are being used. Also e-commerce, which is now one of the most popular ways to trade deals with the same problems, as many dexterous find various interception methods to steal information.

ΠΕΡΙΕΧΟΜΕΝΑ

Εισαγωγή

Η ασφάλεια των δικτύων και των υπολογιστών είναι ένα θέμα το οποίο μόνιμα απασχολεί κάθε διαχειριστή δικτύων. Από τη μια πλευρά οι επιχειρήσεις αυξάνουν την διασύνδεσή τους με το Internet, πχ μέσω χρήσης στατικών IP διευθύνσεων, με ανάπτυξη και δημοσίευση εταιρικού περιεχομένου (πχ web email, portals, web εφαρμογές) στο διαδίκτυο κλπ. Από την άλλη οι hackers, spammers, συγγραφείς κακόβουλου λογισμικού όπως virus, trojans, scripts κλπ διαρκώς αυξάνουν τις επιθέσεις, δημιουργούν νέους κινδύνους στα εταιρικά περιβάλλοντα και βρίσκουν νέους τρόπους παράκαμψης των συστημάτων ασφαλείας.

Πως αντιδρούν οι εταιρίες στις προκλήσεις αυτές; Δυστυχώς ένας μεγάλος αριθμός εταιριών παίρνουν ελάχιστα ή τα απολύτως στοιχειώδη μέτρα, θεωρώντας ότι τα δεδομένα τα οποία διαχειρίζονται δεν έχουν τέτοια αξία ώστε κάποιος hacker να ασχοληθεί μαζί τους για να τα κλέψει ή να τα καταστρέψει. Δεν συνειδητοποιούν όμως ότι ένας "εκπαιδευόμενος" hacker ή συγγραφέας κακόβουλου λογισμικού επιλέγει κατ' αρχάς εύκολα περιβάλλοντα προκειμένου να ξεκινήσει τις επιθέσεις του ώστε να αποκτήσει εμπειρία και φήμη στη κοινότητά του. Ακόμη περισσότερο, οι hackers τις περισσότερες φορές δεν ενδιαφέρονται για συγκεκριμένες εταιρίες-στόχους, αλλά ξεκινούν σαρώνοντας ένα εύρος IP διευθύνσεων ώστε να βρουν αυτές στις οποίες μπορούν να διεισδύσουν. Πολλοί hackers δεν έχουν κατ' ανάγκη οικονομικά κίνητρα, αλλά μπορεί να δρουν έτσι ώστε να έχουν τη "χαρά" ότι έχουν τη δυνατότητα να παραβιάσουν κωδικούς, συστήματα ασφαλείας, και να θέσουν ένα δίκτυο υπό τον έλεγχό τους. Από την άλλη, οι "επαγγελματίες" μπορεί να χρησιμοποιήσουν ένα πλημμελώς προστατευόμενο σύστημα προκειμένου να ξεκινήσουν από εκεί επιθέσεις σε άλλα, να στείλουν μαζικά (spam) emails από τον mail server του συστήματος αυτού και άλλες ενέργειες στις οποίες το ελεγχόμενο σύστημα φαίνεται ως "επιτιθέμενο" με αποτέλεσμα σοβαρές επιπτώσεις και στη φήμη της εταιρίας.

Σήμερα υπάρχει πληθώρα πληροφόρισης και εργαλείων τα οποία μπορεί να χρησιμοποιήσει ο οποιοσδήποτε ώστε να διαπιστώσει και να εκμεταλευτεί τις αδυναμίες ενός δικτύου. Έτσι τώρα ακόμη περισσότερο από ποτέ, καθώς είναι εύκολο ακόμη και για τον πλέον αρχάριο στο hacking να σκανάρει, να διεισδύσει και

να προσβάλει να συστήματά μας, καθίσταται πολύ σημαντικό να έχουμε τους κατάλληλους συμβούλους στα θέματα ασφαλείας. Διότι, όπως συμβαίνει και με τις περισσότερες καταστάσεις, το κόστος της πρόληψης είναι πολύ μικρότερο από το κόστος της αποκατάστασης, και στο συγκεκριμένο θέμα κάποιες φορές μπορεί να αφορά τη φήμη της εταιρίας ώστε η πλήρης αποκατάσταση να μην είναι εφικτή.

Κεφάλαιο 1^{ο} : Ασφάλεια του Εξυπηρέτη Web

1.1 Σφάλματα στην ασφάλεια του Εξυπηρέτη Web

Ο εξυπηρέτης web πρέπει να προστατευτεί τόσο από τους εσωτερικούς χρήστες του δικτύου, στο οποίο ανήκει, όσο και από τους εξωτερικούς χρήστες που επιδιώκουν να συνδεθούν μαζί του. Το σύστημα προστασίας που θα εφαρμοστεί εξαρτάται από την εσωτερική διαμόρφωση του εξυπηρέτη, όπως επίσης και από τις απαιτήσεις των root directories και τις άδειες που δίνονται στους χρήστες.

Τη διαμόρφωση του εξυπηρέτη Web την αναλαμβάνει συνήθως κάποιος χρήστης/διαχειριστής. Πρέπει να επισημανθεί ότι ένας εξυπηρέτης με κακή διαμόρφωση(configuration) μπορεί να δημιουργήσει προβλήματα ασφάλειας ακόμη και σε ένα πολύ καλά σχεδιασμένο σύστημα ασφάλειας. Για το λόγο αυτό, πρέπει να αναλαμβάνει τη διαχείριση του εξυπηρέτη Web ένα έμπειρο και αξιόπιστο άτομο.

Η ικανότητα των εξυπηρετών Web να ενσωματώνουν CGI scripts περιπλέκει σημαντικά την εφαρμογή ενός συστήματος ασφάλειας. Τα CGI scripts προσθέτουν νέα χαρακτηριστικά και δυνατότητες σε έναν εξυπηρέτη Web. Ταυτόχρονα όμως καθιστούν τον εξυπηρέτη πιο ευαίσθητο σε θέματα ασφάλειας. Για παράδειγμα, ένας εξυπηρέτης Web μπορεί να έχει ρυθμιστεί έτσι ώστε να έχει πρόσβαση σε αρχεία ενός συγκεκριμένου καταλόγου, αλλά ένας χρήστης να εγκαταστήσει, ηθελημένα ή όχι, ένα CGI script που να επιτρέπει την ανάγνωση κάθε αρχείου στον υπολογιστή.

Η σύνταξη των CGI script πρέπει να γίνεται με ιδιαίτερη προσοχή. Οι περισσότεροι χρήστες δεν έχουν εμπειρία στη σύνταξη ασφαλών CGI script και συνεπώς υπάρχει υψηλή πιθανότητα να περιέχουν αδυναμίες, επιτρέποντας έτσι σε εισβολείς να εκτελέσουν οποιαδήποτε εντολή στο σύστημα του εξυπηρέτη Web.

Τα κενά στην ασφάλεια του εξυπηρέτη Web, που δημιουργούνται από τα λάθη ή την άγνοια των χρηστών, μπορεί να έχουν δυσάρεστες συνέπειες τόσο για τον ίδιο τον εξυπηρέτη όσο και για την ακεραιότητα των αρχείων που φυλάσσονται σε αυτόν. Αναφέρονται ενδεικτικά κάποια από τα προβλήματα που είναι πιθανό να παρουσιαστούν:

- Ένας εισβολέας μπορεί να εκμεταλλευτεί ατέλειες (bugs) του εξυπηρέτη Web ή των CGI script για να αποκτήσει μη εγκεκριμένη πρόσβαση σε αρχεία του

εξυπηρέτη, να επέμβει στον εξυπηρέτη τροποποιώντας το σύστημα, να θέσει τον εξυπηρέτη σε προσωρινή αχρηστία ή ακόμα και να αποκτήσει τον έλεγχο ολόκληρου του υπολογιστή.

- Εμπιστευτικές πληροφορίες που βρίσκονται αποθηκευμένες στον εξυπηρέτη Web μπορεί να διαμενηθούν σε μη εξουσιοδοτημένα άτομα.
- Εμπιστευτικές πληροφορίες που ανταλλάσσονται μεταξύ του εξυπηρέτη Web και του προγράμματος πλοήγησης μπορεί να υποκλαπούν ή να υπάρξει παρεμπόδιση στην αποστολή των δεδομένων, σε οποιοδήποτε σημείο της διαδρομής μεταξύ του εξυπηρέτη και του προγράμματος πλοήγησης.

1.2 Η πολιτική της ασφάλειας

Για την ασφάλεια του εξυπηρέτη Web και κατ' επέκταση για την ασφάλεια όλου του δικτύου, πρέπει να υπάρχει ένα ολοκληρωμένο σύστημα προστασίας. Η υλοποίησή του ανατίθεται στο διαχειριστή του εξυπηρέτη. Το σύστημα ασφάλειας ουσιαστικά δεν είναι τίποτα άλλο παρά μία περίληψη του πως πρέπει να λειτουργεί ο εξυπηρέτης Web, ώστε να ανταποκρίνεται στις απαιτήσεις των χρηστών του. Για την κατασκευή ενός ασφαλούς εξυπηρέτη Web σε οποιαδήποτε πλατφόρμα, πρέπει να ληφθούν υπόψη τα εξής θέματα:

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

Το καθένα από τα παραπάνω απαιτεί τη λήψη ιδιαίτερων μέτρων. Δυστυχώς, κάποια από τα μέτρα που λαμβάνονται είναι αλληλοσυγκρουόμενα. Για παράδειγμα, για να ελαχιστοποιηθεί ο κίνδυνος της παρακολούθησης της επικοινωνίας πολλοί οργανισμοί αγοράζουν ασφαλείς εξυπηρέτες Web, που

βασίζονται σε κρυπτογραφικά πρωτόκολλα. Αλλά τέτοιοι εξυπηρέτες απαιτούν ψηφιακά υπογεγραμμένα πιστοποιητικά για να λειτουργήσουν και τα πιστοποιητικά αυτά πρέπει να ανανεώνονται τακτικά γεγονός που καθιστά τους εξυπηρέτες ευάλωτους στις λεγόμενες επιθέσεις ‘’άρνησης υπηρεσίας’’(denial of service attacks ή DoS attacks).

Οι επιθέσεις ‘’άρνησης υπηρεσίας’’ σχεδιάστηκαν με σκοπό να καταστήσουν τον υπολογιστή ή το δίκτυο ανίκανο να επιτελέσει τις συνηθισμένες του λειτουργίες. Συνήθως έχουν ως στόχο το εύρος ζώνης ή τη σύνδεση του δικτύου, όπου ανήκει ο υπολογιστής. Οι επιθέσεις με στόχο το εύρος ζώνης κατακλύζουν το δίκτυο με τόσο φόρτο που οι διαθέσιμες πηγές του ξοδεύονται και οι αιτήσεις των χρηστών δεν ικανοποιούνται. Οι επιθέσεις στη σύνδεση κατακλύζουν το δίκτυο με μεγάλο αριθμό αιτήσεων για σύνδεση, με αποτέλεσμα οι διαθέσιμες πηγές του συστήματος να καταναλώνονται και το σύστημα να μη μπορεί πλέον να ικανοποιήσει τις νόμιμες αιτήσεις των χρηστών του.

Η πολιτική της ασφάλειας, που θα εφαρμοστεί, για την υλοποίηση του συστήματος προστασίας είναι καλό να συμπεριλάβει και παράγοντες όπως:

- Ποιοι επιτρέπεται να χρησιμοποιούν το σύστημα
- Πότε επιτρέπεται να το χρησιμοποιούν
- Τι επιτρέπεται να κάνουν

Είναι πιθανό διαφορετικές ομάδες χρηστών να έχουν διαφορετικά δικαιώματα εισόδου στα διάφορα μέρη του εξυπηρέτη Web. Επίσης, οι διαδικασίες παροχής εισόδου στο σύστημα και οι διαδικασίες ανάκλησης της εισόδου, όταν για παράδειγμα ένας χρήστης φεύγει από το σύστημα, αποτελούν ένα σημαντικό κομμάτι του συστήματος προστασίας.

Ένα ακόμη σημείο το οποίο πρέπει να ληφθεί υπόψη είναι το πώς ορίζεται η αποδεκτή χρήση του συστήματος. Ακόμη στο σύστημα προστασίας, πρέπει να συμπεριληφθούν οι μέθοδοι εισόδου (login) σε αυτό, τόσο για τους εσωτερικούς όσο και για τους εξωτερικούς χρήστες. Τέλος, ιδιαίτερο βάρος πρέπει να δοθεί στα πρωτόκολλα που αφορούν στις αντιδράσεις του συστήματος σε τυχόν κενά ασφαλείας.

Τελικά, τόσο οι χρήστες του Διαδικτύου όσο και οι διαχειριστές των εξυπηρετών web έχουν λόγους να ανησυχούν για την ασφάλεια των δεδομένων που μεταφέρονται μέσω του δικτύου. Το πρωτόκολλο επικοινωνίας TCP/IP δεν έλαβε υπόψη θέματα ασφάλειας δικτύου κατά το σχεδιασμό του. Αυτό έχει ως αποτέλεσμα να δημιουργούνται προβλήματα ασφάλειας στη μετάδοση εμπιστευτικών εγγράφων από τον εξυπηρέτη προς το πρόγραμμα πλοήγησης του χρήστη ή ακόμη και στην αποστολή προσωπικών πληροφοριών του χρήστη πίσω στον εξυπηρέτη.

1.3 Ασφάλεια των συστημάτων και λογισμικού των Εξυπηρετών Web

Στο εμπόριο και στο Διαδίκτυο υπάρχουν πολλά λειτουργικά συστήματα. Μερικά από αυτά είναι πιο ασφαλή και μπορούν να χρησιμοποιηθούν ως πλατφόρμες για εξυπηρέτες Web. Όσο πιο ευέλικτο και δυναμικό είναι ένα σύστημα τόσο πιο ευάλωτο είναι στις επιθέσεις κατά του εξυπηρέτη. Επίσης, όσα περισσότερα χαρακτηριστικά χρήσης και ευκολίας προσφέρει ο εξυπηρέτης τόσο πιο πιθανό είναι να περιέχει κενά στην ασφάλειά του.
Η εμπειρία έχει δείξει ότι το πιο σίγουρο σύστημα για εξυπηρέτη Web είναι ένας υπολογιστής που τρέχει αποκλειστικά τον εξυπηρέτη και καμία άλλη εφαρμογή. Οι απλοί εξυπηρέτες που περιέχουν μόνο τα στατικά αρχεία αιτήσεων και καμία άλλη εφαρμογή θεωρούνται ασφαλέστεροι από τους περίπλοκους εξυπηρέτες που εκτελούν CGI scripts, υποστηρίζουν τις απομακρυσμένες συνδέσεις, έχουν έτοιμη για χρήση scripting language και προσφέρουν χαρακτηριστικά όπως η λίστα των directories ή τα περιεχόμενα του εξυπηρέτη.
Λόγω: α) της πληθώρας των γλωσσών προγραμματισμού, β) των εσωτερικά σε αυτό εγκαταστημένων εξυπηρετών, γ) της πλούσιας ποικιλίας εργαλείων και δ) της ικανότητας σύνδεσης πολλών χρηστών την ίδια στιγμή από οποιοδήποτε απομακρυσμένο σημείο του Διαδικτύου, το λειτουργικό σύστημα UNIX θεωρείται ως μη βέλτιστη επιλογή για εξυπηρέτη Web. Επειδή υπάρχουν πολλοί τρόποι εισόδου στο σύστημα, είναι εύκολο για τους εισβολείς να εισβάλουν σε αυτό.

Με το σκεπτικό αυτό, λιγότερο ικανά συστήματα, με περιορισμένα εργαλεία και ευκολίες, όπως τα MS-WINDOWS και τα MACINTOSH, είναι δυσκολότερο να δεχτούν επίθεση και επομένως είναι πιο κατάλληλα για εξυπηρέτες Web. Βέβαια, το σύστημα UNIX είναι πιο γρήγορο λειτουργικό από το MacOS και είναι διαθέσιμο για πλατφόρμες που είναι πιο γρήγορες από αυτές που χρησιμοποιούν MS-WINDOWS.

Όσοι επιλέγουν να τρέξουν έναν εξυπηρέτη Window NT ή UNIX έχουν τα πλεονεκτήματα που προσφέρει ένα σύστημα πολυπρογραμματισμού (multitasking) και το κέρδος μίας ενδιάμεσης σύνδεσης ή της σύνδεσης με μία βάση δεδομένων. Φυσικά, υπάρχουν προβλήματα στην ασφάλεια των συστημάτων αυτών και θα συνεχίσουν να υπάρχουν. Στο σύνολό τους τα Windows NT είναι τρωτά. Αυτό συμβαίνει γιατί το σύστημα οργάνωσης τους είναι σχετικά καινούριο και τα μεγάλα κενά στην ασφάλεια δεν έχουν εμφανιστεί ακόμα αλλά και επειδή το σύστημα αρχείων NT και το σύστημα λογαριασμών των χρηστών είναι αρκετά περίπλοκο και δύσκολο να ρυθμιστεί σωστά.

Ο περιορισμός των λογαριασμών εισόδου (login) που είναι διαθέσιμοι στο σύστημα, η διαγραφή των μη ενεργών χρηστών, τα passwords των προνομιούχων λογαριασμών, το κλείσιμο των μη απαραίτητων ή μη χρησιμοποιούμενων υπηρεσιών του συστήματος, ο συχνός έλεγχος των αρχείων πρόσβασης (log files) του εξυπηρέτη και του συστήματος για ύποπτες ενέργειες και η κατάλληλη προσοχή στις άδειες των χρηστών είναι μερικές από τις προφυλάξεις που πρέπει να λαμβάνονται όταν οι εξυπηρέτες web τρέχουν σε περιβάλλον UNIX ή NT.

Σε ένα καλά οργανωμένο περιβάλλον, όπου οι κανόνες ασφάλειας έχουν ρυθμιστεί με τον καλύτερο δυνατό τρόπο και τηρούνται πιστά, ένα τυπικό σύστημα UNIX είναι ασφαλέστερο από ένα σύστημα NT. Τέλος, ένας από τους σημαντικότερους παράγοντες που επηρεάζουν το σύστημα και την ασφάλεια του είναι το προσωπικό που είναι υπεύθυνο για τον εξυπηρέτη και το λογισμικό. Ένα σύστημα UNIX το οποίο διαχειρίζεται ένας έμπειρος χρήστης είναι πιο ασφαλές από ένα MS-WINDOWS σύστημα που διαχειρίζεται ένας αρχάριος.

1.4 Μέτρα Ασφαλείας

Χρήση του μηχανήματος μόνο ως Εξυπηρέτη Web

Όταν ένας υπολογιστής χρησιμοποιείται αποκλειστικά ως εξυπηρέτης Web, η ασφάλεια του δικτύου αυξάνεται. Κάτι τέτοιο κάνει πιο δύσκολη την έναρξη «επιτυχημένης» επίθεσης κατά του μηχανήματος. Αλλά ακόμα και αν το μηχάνημα ‘’καταληφθεί’’, ο εισβολέας δε θα μπορεί να κάνει επιπλέον ζημιά στο δίκτυο. Στην περίπτωση ενός υπολογιστή που λειτουργεί μόνο ως εξυπηρέτης Web, συνιστάται η υιοθέτηση των παρακάτω κανόνων:

- Διαγραφή όλων των άχρηστων λογαριασμών.
- Διαγραφή όλων των μεταφραστών γλωσσών(compilers).
- Διαγραφή όλων των προγραμμάτων που δε χρησιμοποιούνται από τον εξυπηρέτη Web ή από το λογισμικό του μηχανήματος κατά την εκκίνησή του.
- Παροχή των απαιτούμενων υπηρεσιών και μόνο αυτών.
- Μη υποστήριξη υπηρεσιών εξυπηρέτη ηλεκτρονικού ταχυδρομείου(e-mail server).
- Αποφυγή χρήσης καταλόγων από το Σύστημα Αρχείων Δικτύου (Network File System, NFS).

Μία άλλη φιλοσοφία στην εγκατάσταση του εξυπηρέτη Web είναι η τοποθέτηση όλων των αρχείων του σε μια ξεχωριστή δομή καταλόγων, με τη χρήση της εντολής **chroot**. Όλο το υπόλοιπο σύστημα αρχείων παραμένει κρυφό από τον εξυπηρέτη Web, ο οποίος δε γνωρίζει καν την ύπαρξή του, γεγονός που περιορίζει μία πιθανή επίθεση στους καταλόγους του εξυπηρέτη.

Κεφάλαιο 2^{ο} : Ασφάλεια του χρήστη

2.1 Βασικές έννοιες και όροι ασφάλειας στο επίπεδο του χρήστη

- **Broadcasting (Ευρεία εκπομπή):** Μέθοδος αποστολής του ίδιου μηνύματος σε όλους τους υπολογιστές ενός υποδικτύου, ταυτόχρονα. Παρόμοια έννοια είναι το multicasting (πολλαπλή εκπομπή), μόνο που τώρα οι παραλήπτες του μηνύματος είναι προεπιλεγμένοι όχι κατ' ανάγκη όλοι οι υπολογιστές.
- **Firewall (φράγμα ασφάλειας):** Μέθοδος προστασίας που υλοποιείται σε επίπεδο υλικού ή/και λογισμικού και χρησιμοποιείται για να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση από και προς ένα δίκτυο. Συχνά τα φράγματα ασφάλειας χρησιμοποιούνται για να εμποδίζουν χρήστες του Διαδικτύου να προσπελάζουν ιδιωτικά δίκτυα, τα οποία είναι και αυτά συνδεδεμένα με το Διαδίκτυο. Γενικά, μπορούμε να πούμε ότι ένα φράγμα ασφάλειας διαχωρίζει ένα δίκτυο από κάποιο άλλο.
- **Hub:** Κοινό σημείο σύνδεσης για ένα πλήθος υπολογιστών σε ένα τοπικό δίκτυο (τοπολογία αστέρα). Ένα hub έχει πολλές θύρες (ports). Όταν ένα πακέτο φτάνει σε μία θύρα, αντιγράφεται σε όλες τις άλλες, με αποτέλεσμα όλοι οι υπολογιστές που είναι συνδεδεμένοι με το hub να ‘’βλέπουν’’ όλα τα διακινούμενα πακέτα. Σε αντιδιαστολή βρίσκονται τα διακοπτικά στοιχεία τοπικών υπολογιστών ή πλαισίων: κάθε φορά που ένα πακέτο φτάνει σε μία θύρα, διαβάζεται η διεύθυνση προορισμού στην κεφαλή του και το πακέτο προωθείται μόνο στη θύρα στην οποία αντιστοιχεί ο υπολογιστής με τη συγκεκριμένη διεύθυνση.
- **ICMP (Internet Control Message Protocol):** Επέκταση του πρωτοκόλλου IP για την αποστολή μηνυμάτων λαθών και ελέγχου. Χρησιμοποιείται από την εντολή Ping για να διαπιστώνεται, μεταξύ των άλλων, εάν ένα μηχάνημα είναι ενεργό, από δρομολογητές (routers), κάθε φορά που ειδοποιούν ένα μηχάνημα για τη μη διαθεσιμότητα ενός κόμβου στον οποίο απευθύνονται κτλ.
- **IP Spoofing:** Τεχνική για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε δικτυωμένα μηχανήματα. Ο εισβολέας αποστέλλει μηνύματα με διευθύνσεις

IP που υποδεικνύουν ότι αυτά προέρχονται από ένα ‘’έμπιστο’’ port.Ο επίδοξος cracker αρχικά καταφεύγει σε ένα πλήθος τεχνικών για να βρει μία διεύθυνση IP που αντιστοιχεί σε μια τέτοια θύρα. Η κατάλληλη ρύθμιση δρομολογητών και φραγμάτων ασφάλειας μπορεί να αποτρέψει τις επιθέσεις του είδους.

- **PING (Packet InterNet Groper):** Εργαλείο για να διαπιστώνεται εάν μια δεδομένη διεύθυνση IP είναι προσβάσιμη. Το πρόγραμμα στέλνει ένα πακέτο σε μια διεύθυνση και στη συνέχεια αναμένει μια απάντηση από τον υπολογιστή στον οποίο αντιστοιχεί αυτή η διεύθυνση.
- **Port Number (αριθμός θύρας):** Αριθμός που αντιστοιχεί σε μια εφαρμογή στο ρόλο διακομιστή, σε ένα δίκτυο βασισμένο στο TCP/IP (όπως, π.χ., το Διαδίκτυο). Η θύρα μπορεί να θεωρηθεί ως το άκρο μιας λογικής σύνδεσης (δηλαδή μιας σύνδεσης όπως τη βλέπει ο χρήστης). Ένας αριθμός θύρας χρησιμοποιείται ώστε εισερχόμενα δεδομένα να αντιστοιχίζονται στην κατάλληλη υπηρεσία (service). Γνωστά παραδείγματα αποτελούν τα port 80, 25 και 20, που χρησιμοποιούνται από διακομιστές ιστοσελίδων, αλληλογραφίας και FTP, αντίστοιχα (www.isi.edu/in-notes/iana/assignments/port-numbers). Ο συνδυασμός μιας διεύθυνσης IP ενός μηχανήματος με έναν αριθμό port ονομάζεται Socket.
- **Promiscuous Mode (Αδιάκριτος Τρόπος Λειτουργίας):** Δικτυωμένος υπολογιστής ρυθμισμένος ώστε να αναγνωρίζει και να δέχεται όλα τα πακέτα που φτάνουν ή περνούν από αυτόν, ανεξαρτήτως πρωτοκόλλου ή προορισμού. Κάθε εργαλείο λογισμικού που χρησιμοποιείται για το φιλτράρισμα δικτυακών πακέτων πρέπει να είναι εγκατεστημένο σε έναν υπολογιστή με κάρτα δικτύου και οδηγούς που το επιτρέπουν να βρίσκεται σε αδιάκριτο τρόπο λειτουργίας.
- **Subnet (υποδίκτυο):** Υποσύνολο ενός δικτύου που περιλαμβάνει υπολογιστές οι οποίοι έχουν διευθύνσεις με ένα κοινό τμήμα. Στα δίκτυα TCP/IP, οι υπολογιστές ενός υποδικτύου έχουν διευθύνσεις IP με κοινό πρόθεμα. Η υποδιαίρεση ενός δικτύου σε υποδίκτυα είναι χρήσιμη τόσο για λόγους ευκολίας διαχείρισης όσο και για λόγους ασφαλείας.

2.2 Ιοί και Σκουλήκια

Οι **Ιοί** είναι ένας βλαβερός κώδικας, ο οποίος επιζεί μόνο με το να "κολλάει" ή να περιέχεται μέσα σε ένα άλλο πρόγραμμα ή σε ένα αρχείο. Στην ουσία οι ιοί αποτελούν και αυτοί ένα λογισμικό / πρόγραμμα, το οποίο όμως δεν μπορεί να υπάρξει αυτόνομα, σαν ξεχωριστό πρόγραμμα. Οι ηλεκτρονικοί ιοί, λοιπόν, επιζούν με το να "μολύνουν" άλλα αρχεία, έχουν δηλαδή την ίδια παρασιτική συμπεριφορά που έχουν και οι οργανικοί ιοί! Ο σκοπός τους βέβαια, μετά την επιβίωση και ανάλογα με τον τρόπο που έχουν προγραμματιστεί, είναι καταστροφικός. Υπάρχουν διαφόρων ειδών ιοί, κάποιοι είναι αρκετά καταστροφικοί και άλλοι λιγότερο.

Συνήθως κολλάμε ιούς ανοίγοντας κάποιο συνημμένο σε email ή επισκέπτοντας μια επικίνδυνη σελίδα στο διαδίκτυο χωρίς να έχουμε θέσει τις κατάλληλες ρυθμίσεις ασφαλείας στον περιηγητή μας (Internet Explorer). Υπάρχουν βέβαια και άλλοι τρόποι με τους οποίους μεταδίδονται οι ιοί, γενικά με οποιονδήποτε τρόπο προϋποθέτει μεταφορά πληροφοριών μεταξύ του Η/Υ και κάποιας άλλης πηγής πχ usb stick, cd-rom, dvd-rom, δισκέτα κτλ. Γι΄αυτό το πρόγραμμα που καταπολεμά τους ιούς (Antivirus) δεν πρέπει να λείπει από κανένα Η/Υ.

Το Antivirus αποτελείται συνήθως από δύο επιμέρους προγράμματα: τον "Φύλακα" (Guard) αλλιώς On-Access-Scan και το κυρίως πρόγραμμα On-Demand-Scan. Ο Φύλακας είναι ανοικτός καθόλη την διάρκεια της λειτουργίας του Η/Υ και ελέγχει όλα τα αρχεία που χρησιμοποιούμε και τις πληροφορίες που κατεβάζουμε από το ίντερνετ για τυχόν ιούς και άλλα βλαβερά λογισμικά. Το κυρίως πρόγραμμα ανοίγει όταν ο φύλακας εντοπίσει κάτι και μας ζητηθεί να επιλέξουμε τι πρέπει να συμβεί με το βλαβερό πρόγραμμα (malware). Οι επιλογές που έχουμε συνήθως είναι είτε να αγνοήσουμε την προειδοποίηση του Antivirus, είτε να διαγράψουμε το αρχείο, είτε να το επισκευάσουμε. Επειδή όμως πάντα υπάρχει η πιθανότητα λάθους, καλό είναι να ελέγχετε αν το ύποπτο πρόγραμμα είναι πραγματικά κακόβουλο ή πρόκειται για μια λάθος εκτίμηση του Antivirus (False Positive). Ο καλύτερος τρόπος να διαπιστώσουμε αν ένα πρόγραμμα είναι κακόβουλο (αν φυσικά δε το αναγνωρίζουμε σαν ένα πρόγραμμα που εγκαταστήσαμε εμείς στον υπολογιστή μας) είναι να ελέγξουμε το αρχείο με ένα άλλο online antivirus. Ένα false positive alarm διορθώνεται συνήθως με την αμέσως επόμενη ενημέρωση.

Τα **σκουλήκια (worms)** είναι και αυτά βλαβερά προγράμματα τα οποία όμως έχουν κάποιες διαφορές από τους ιούς. Ενώ οι ιοί δε μπορούν να υπάρξουν ανεξάρτητοι, τα σκουλήκια αποτελούν ξεχωριστά προγράμματα με μόνο στόχο τον πολλαπλασιασμό τους μέσω της αντιγραφής του εαυτού τους και την αποστολή τους σε όσους περισσότερους Η/Υ γίνεται μέσω του διαδικτύου. Δεν είναι τόσο καταστροφικά όσο οι ιοί γιατί δεν σβήνουν αρχεία, όμως κάνουν τη σύνδεση στο ίντερνετ πιο αργή επειδή στέλνουν τα αντίγραφα τους σε άλλους Η/Υ. Επίσης κάνουν το σύστημα του Η/Υ πιο αργό χρησιμοποιώντας πολύ μνήμη με το να αντιγράφουν τον εαυτό τους άπειρες φορές και γεμίζοντας τον ελεύθερο χώρο του σκληρού δίσκου (rabbits). Υπάρχουν όμως και ορισμένα σκουλήκια που έχουν ταυτόχρονα ιδιότητες ιών, πράγμα που τα καθιστά πιο επικίνδυνα από τα συνηθισμένα σκουλήκια.

Οι **δούρειοι ίπποι** εισβάλλουν στον Η/Υ κρυμμένοι μέσα σε ένα άλλο πρόγραμμα ή παιχνίδι και με ύπουλο τρόπο, όπως στο μυθικό πόλεμο της Τροίας, καταστρέφουν αλλά κυρίως παρακολουθούν. Τα περισσότερα κατασκοπευτικά προγράμματα αποτελούνται από Δούρειους Ίππους η αφαίρεση των οποίων είναι πολλές φορές πιο δύσκολη από την αφαίρεση απλών Troyan.

Δεν θα ήταν υπερβολή αν λέγαμε ότι ο μεγαλύτερος κίνδυνος μετά τους ιούς για την πλειονότητα των χρηστών του Διαδικτύου, προέρχεται από τους ‘’**Δούρειους Ίππους**’’ (Trojan horses).Από τη στιγμή που ένας δούρειος ίππος θα εγκατασταθεί και θα **ενεργοποιηθεί**, κατασκοπεύει την κάθε μας κίνηση και την αναφέρει στον δημιουργό του. Οι **Keyloggers** καταγράφουν και αποθηκεύουν ό,τι πληκτρολογούμε και το στέλνουν στον ιδιοκτήτη του δούρειου ίππου. Έτσι πολύ εύκολα αποκαλύπτονται κωδικοί, αριθμοί πιστωτικών καρτών κτλ πράγμα ιδιαίτερα επικίνδυνο για όσους κάνουν online-banking. Ο δούρειος ίππος μετατρέπεται εύκολα σε **backdoor** (εισβάλλει από την "πίσω πόρτα" του Η/Υ - κερκόπορτα) όταν είναι έτσι σχεδιασμένος ώστε να επιτρέπει στον δημιουργό του να πάρει τον **πλήρη έλεγχο** του Η/Υ που έχει μολύνει.

Η συμπεριφορά ενός online υπολογιστή που είναι μολυσμένος με ένα ενεργοποιημένο backdoor φαίνεται αλλόκοτη στους ανυποψίαστους. Παράθυρα ανοίγουν και κλείνουν. Ο υπολογιστής γίνεται πολύ αργός, τα antivirus και τα firewall απενεργοποιούνται. Ένας τέτοιος **παραβιασμένος** Η/Υ δεν είναι πλέον αξιόπιστος και η μόνη λύση για να εξαληφθούν όλα τα ίχνη των ιών είναι το format. Αν έχετε

μολυνθεί με backdoor ή troyan, πρέπει άμεσα να αλλάξετε τους κωδικούς σας (σε όλα τα site που επισκέπτεστε) γιατί 99% θα έχουν περάσει στην κατοχή τρίτων.

Δούρειους Ίππους κολλάμε συνήθως από το ίντερνετ, υπάρχει όμως περίπτωση να εγκατασταθεί έναν troyan από κάποιον ο οποίος έχει φυσική πρόσβαση στον Η/Υ. Γιαυτό είναι σκόπιμο να μην αφήνετε τον Η/Υ ανοιχτό χωρίς ένα screensaver με password. Επίσης μην αφήνετε χαρτιά και σημειώσεις με τους κωδικούς σας κοντά στον Η/Υ. Ακόμα πιο σημαντικό είναι να μην αποθηκεύετε τους κωδικούς σας σε αρχεία κειμένου, εκτός και αν τα κρυπτογραφείτε με ισχυρά password και τα κλειδώνετε σε zip.

2.3 Ασπίδες Προστασίας

Παρά την ύπαρξη ενός μεγάλου αριθμού ιών, ο κίνδυνος ‘’μόλυνσης’’ μπορεί να ελαχιστοποιηθεί αν τηρηθούν μερικοί βασικοί κανόνες. Εκτός από την αναβάθμιση των εφαρμογών που σχετίζονται με το Διαδίκτυο, είναι πλέον επιβεβλημένη η εγκατάσταση στον υπολογιστή κάποιας εφαρμογής προστασίας από τους ιούς. Μετά την εγκατάσταση θα πρέπει να γίνεται εβδομαδιαία ενημέρωση από τους δημιουργούς (μέσω Διαδικτύου κατά προτίμηση), ώστε να υπάρχει αυξημένο επίπεδο προστασίας απέναντι και στους νεότερους των ιών.

Με την εγκατάσταση ενός Προγράμματος Αντιμετώπισης Ιών (Antivirus) σε έναν υπολογιστή, μειώνεται δραματικά η πιθανότητα εισβολής κάποιου ιού, σκουληκιού ή δούρειου ίππου. Με κανέναν όμως τρόπο δεν αποτρέπονται οι κακόβουλοι crackers από το να δοκιμάσουν να διεισδύσουν στον υπολογιστή. Για να εξασφαλιστεί η μέγιστη δυνατή προστασία, θα πρέπει να εγκατασταθεί στον προσωπικό υπολογιστή κάποιο φράγμα ασφαλείας.

Εάν υπάρχει μόνιμη σύνδεση με το Διαδίκτυο (και κατά συνέπεια σταθερό IP), εάν ο υπολογιστής υποστηρίζει εξυπηρέτες (π.χ., Web server) ή απομακρυσμένη πρόσβαση (PC Anywhere-Wingate κ.λ.π.) ή απλώς θέλουμε να ελέγχουμε τι έρχεται και τι φεύγει από το PC μας, θα πρέπει να εγκαταστήσουμε ένα φράγμα ασφάλειας. Πρόκειται για μια ειδική εφαρμογή που απομονώνει το σύστημά μας από το Διαδίκτυο και στην ουσία το καθιστά μη ‘’ορατό’’ για τον έξω κόσμο, ακόμα και αν είναι on-line.Επιπλέον, με βάση κάποιους συγκεκριμένους κανόνες, ελέγχει και κατά

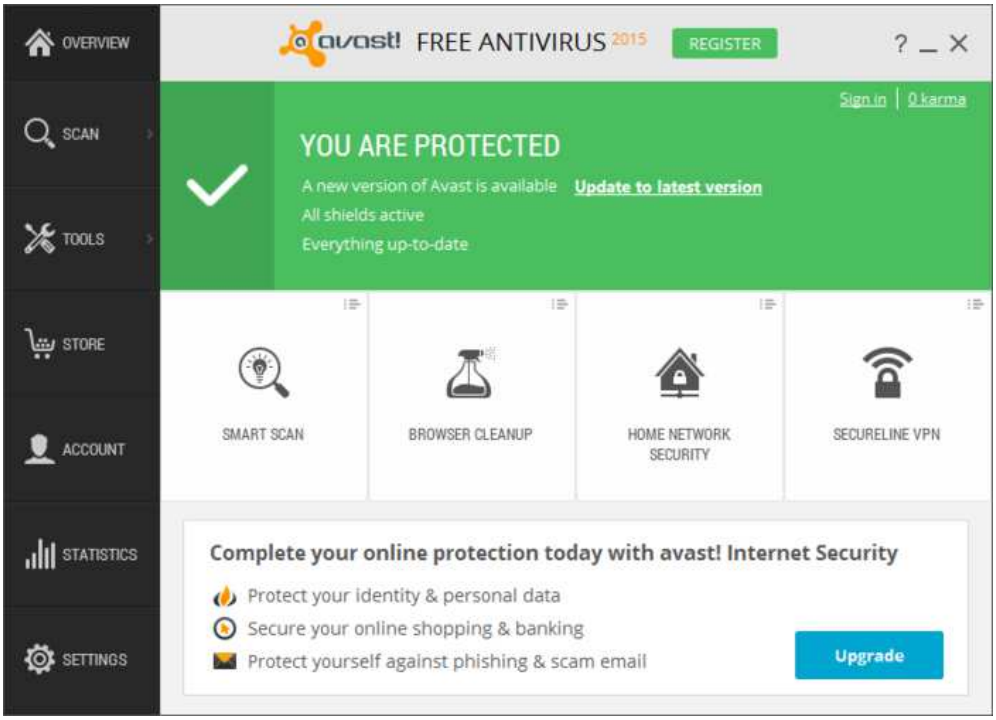
συνέπεια επιτρέπει ή εμποδίζει να εισέλθουν στο σύστημα ή να εξέλθουν από αυτό τα πακέτα δεδομένων του Διαδικτύου.

2.4 Προσωπικά Φράγματα Ασφάλειας (Firewalls)

Παρακάτω παρουσιάζονται κάποια από τα πιο γνωστά προσωπικά φράγματα ασφάλειας. Είναι σημαντικό να τονιστεί ότι κανένα από αυτά δεν προσφέρουν απόλυτη προστασία. Ιδιαίτερα ισχυρά (και ακριβά) σχήματα προστασίας έχουν κατά καιρούς αποτύχει.

Avast

Δωρεάν έκδοση ενός ισχυρού προγράμματος προστασίας από ιούς. Ανανεώνεται σε τακτά χρονικά διαστήματα μέσω του διαδικτύου. Ορισμένοι χρήστες έχουν δηλώσει ότι χρησιμοποιεί υπερβολικά πολλή από την υπολογιστική δύναμη του επεξεργαστή, επιβαρύνοντας έτσι τη λειτουργία του υπολογιστή, παρόλα ταύτα είναι ένα ολοκληρωμένο εργαλείο προστασίας με πάρα πολύ καλά αποτελέσματα.

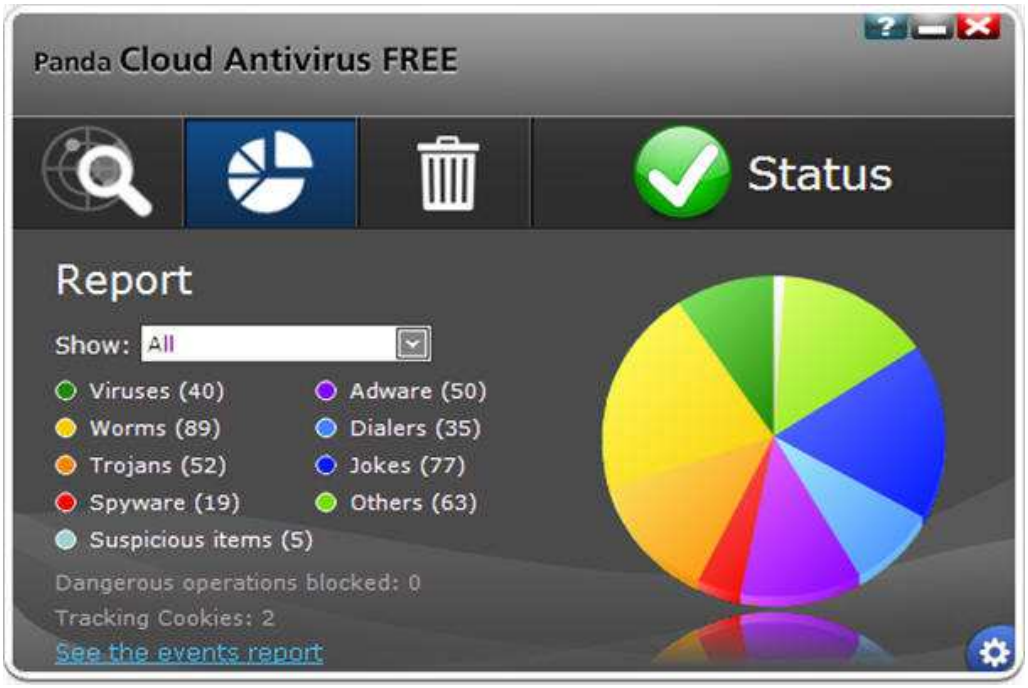


AVG Free

Ένα πανίσχυρο πρόγραμμα προστασίας από ιούς. Διαθέτει ασπίδα προστασίας που λειτουργεί σε πραγματικό χρόνο και λαμβάνει την ενημέρωση του από το διαδίκτυο. Διατίθεται δωρεάν μόνο για ιδιωτική χρήση. Ένα από τα καλύτερα προγράμματα προστασίας του υπολογιστή μας και ένα από τα καλύτερα anti-virus στον κόσμο.

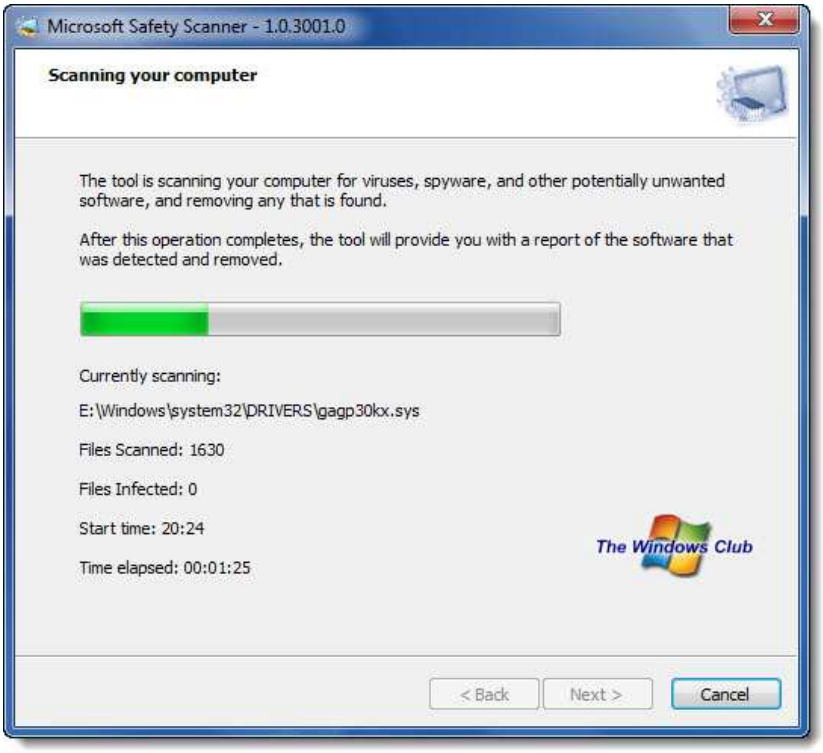
Panda Cloud Antivirus

Ένα δωρεάν πακέτο προστασίας του υπολογιστή μας από την εταιρία Panda.Πρόκειται για μια από τις πιο αξιόπιστες εταιρίες στον χώρο της αντιμετώπισης ιών και άλλων απειλών. Το Cloud είναι το πρώτο δωρεάν πακέτο από την εταιρία και υπόσχεται πολλά.



Microsoft Safety Scanner

Εφαρμογή από τη MicroSoft που ανιχνεύει τον υπολογιστή μας για ιούς και μας βοηθάει να τον καθαρίσουμε στην περίπτωση που κάτι βρεθεί. Δεν πρόκειται για ασπίδα προστασίας σε πραγματικό χρόνο και δεν αντικαθιστά το παραδοσιακό antivirus, αλλά το συμπληρώνει. Η εφαρμογή μπορεί να εκτελεστεί μέχρι και δέκα μέρες αφού την κατεβάσουμε ξανά, κάτι το οποίο εγγυάται ότι χρησιμοποιούμαι μια πρόσφατα ενημερωμένη έκδοση. Υποστηρίζει λειτουργικά Windows μόνο.


Microsoft Safety Scanner - 1.0.3001.0
Scanning your computer
The tool is scanning your computer for viruses, spyware, and other potentially unwanted software, and removing any that is found.
After this operation completes, the tool will provide you with a report of the software that was detected and removed.
Currently scanning:
E:\Windows\system32\DRIVERS\gagp30kx.sys
Files Scanned: 1630
Files Infected: 0
Start time: 20:24
Time elapsed: 00:01:25
The Windows Club
< Back
Next >
Cancel

Κεφάλαιο 3^{ο} : Ψηφιακές Υπογραφές

3.1 Κρυπτογραφία

Η ανάγκη για εμπιστευτικότητα στην ηλεκτρονική συναλλαγή ικανοποιείται με την κρυπτογραφία. Ο αποστολέας χρησιμοποιώντας κάποια μαθηματική συνάρτηση μετατρέπει το αρχικό κείμενο σε μορφή μη κατανοητή για οποιονδήποτε τρίτο (κρυπτογραφημένο κείμενο). Ο παραλήπτης έχοντας γνώση του τρόπου κρυπτογράφησης, αποκρυπτογραφεί το κείμενο στην αρχική του μορφή. Το μήνυμα παραμένει εμπιστευτικό, μέχρι να αποκρυπτογραφηθεί.

Τα σύγχρονα κρυπτοσυστήματα χρησιμοποιούν αλγόριθμους και κλειδιά (σειρά από bits συγκεκριμένου μήκους) για να διατηρήσουν την πληροφορία ασφαλή.

Μία παραδοσιακή μέθοδος κρυπτογράφησης είναι η **συμμετρική κρυπτογραφία** η οποία χρησιμοποιεί το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση. Ο αποστολέας κρυπτογραφεί και ο παραλήπτης αποκρυπτογραφεί με το ίδιο κλειδί. Το κλειδί θα πρέπει να παραμένει μυστικό και να είναι γνωστό μόνο στους συναλλασσόμενους. Η μέθοδος αυτή παρουσιάζει μειονεκτήματα όσον αφορά την εφαρμογή της σε ανοιχτά δίκτυα με πολλούς χρήστες και τις αυξημένες απαιτήσεις της για την ασφάλεια (π.χ. αποθήκευση των κλειδιών κ.λ.π).

Η **ασύμμετρη κρυπτογραφία** (ή κρυπτογραφία δημοσίου κλειδιού- public key cryptography) χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και την αποκρυπτογράφηση. Κάθε χρήστης έχει στη διάθεσή του δύο κλειδιά. Το δημόσιο κλειδί είναι αυτό που ο χρήστης μπορεί να το γνωστοποιήσει σε τρίτους ενώ το ιδιωτικό είναι εκείνο που το φυλάσσει με ασφάλεια και μόνο αυτός θα πρέπει να το γνωρίζει και κατέχει. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη. Έτσι, το μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη (που είναι ο κάτοχος του αντίστοιχου ιδιωτικού κλειδιού εκτός και αν η μυστικότητα του ιδιωτικού κλειδιού έχει παραβιαστεί).

3.2 Κρυπτογράφηση Δημοσίου Κλειδιού

Η **κρυπτογράφηση δημοσίου κλειδιού (Public Key Cryptography) ή ασύμμετρου κλειδιού (Asymmetric Cryptography)** επινοήθηκε στο τέλος της δεκαετίας του 1970 από τους Whitfield Diffie και Martin Hellman και παρέχει ένα εντελώς διαφορετικό μοντέλο διαχείρισης των κλειδιών κρυπτογράφησης από την προγενέστερη κρυπτογράφηση συμμετρικού κλειδιού. Η βασική ιδέα είναι ότι ο αποστολέας και ο παραλήπτης δεν μοιράζονται ένα κοινό μυστικό κλειδί όπως στην περίπτωση της κρυπτογράφησης συμμετρικού κλειδιού, αλλά διαθέτουν διαφορετικά κλειδιά για διαφορετικές λειτουργίες.

Συγκεκριμένα κάθε χρήστης διαθέτει δύο κλειδιά κρυπτογράφησης: το ένα ονομάζεται **ιδιωτικό κλειδί (private key)** και το άλλο **δημόσιο κλειδί (public key)**. Το ιδιωτικό κλειδί θα πρέπει ο κάθε χρήστης να το προφυλάσσει και να το κρατάει κρυφό, ενώ αντιθέτως το δημόσιο κλειδί μπορεί να το ανακοινώνει σε όλη τη διαδικτυακή κοινότητα ή σε συγκεκριμένους παραλήπτες. Υπάρχουν δε και ειδικοί εξυπηρετητές δημοσίων κλειδιών (public key servers) στους οποίους μπορεί κανείς να απευθυνθεί για να βρει το δημόσιο κλειδί του χρήστη που τον ενδιαφέρει ή να ανεβάσει το δικό του δημόσιο κλειδί για να είναι διαθέσιμο στο κοινό.

Τα δύο αυτά κλειδιά (ιδιωτικό και δημόσιο) έχουν μαθηματική σχέση μεταξύ τους. Εάν το ένα χρησιμοποιηθεί για την κρυπτογράφηση κάποιου μηνύματος, τότε το άλλο χρησιμοποιείται για την αποκρυπτογράφηση αυτού. Η επιτυχία αυτού του είδους κρυπτογραφικών αλγορίθμων βασίζεται στο γεγονός ότι η γνώση του δημόσιου κλειδιού κρυπτογράφησης δεν επιτρέπει με κανέναν τρόπο τον υπολογισμό του ιδιωτικού κλειδιού κρυπτογράφησης.

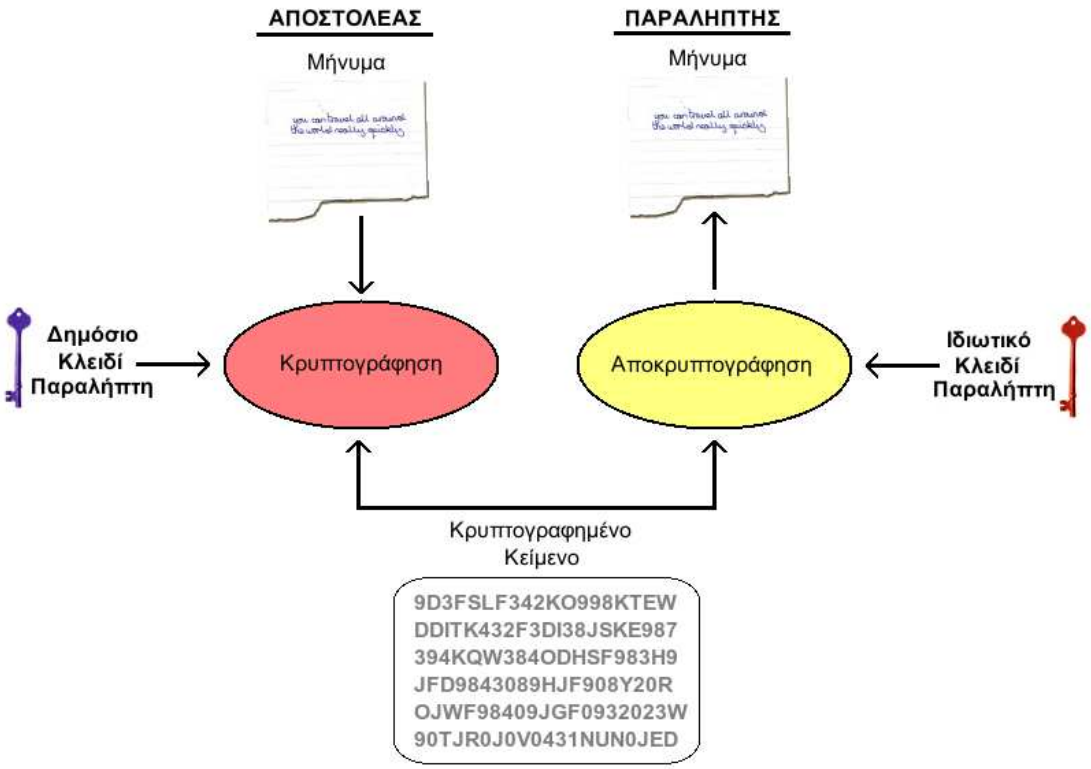
3.2.1 Δημιουργία κλειδιών

Η δημιουργία του δημόσιου και του ιδιωτικού κλειδιού γίνεται από ειδικές συναρτήσεις οι οποίες δέχονται ως είσοδο έναν μεγάλο τυχαίο αριθμό και στην έξοδο παράγουν το ζεύγος των κλειδιών. Είναι προφανές ότι όσο πιο τυχαίος είναι ο αριθμός που παρέχεται ως είσοδος στη γεννήτρια κλειδιών τόσο πιο ασφαλή είναι τα κλειδιά που παράγονται. Σε σύγχρονα προγράμματα κρυπτογράφησης ο τυχαίος αριθμός παράγεται ως εξής: Κατά τη διαδικασία κατασκευής των κλειδιών, το

πρόγραμμα σταματάει για 5 λεπτά και καλεί τον χρήστη να συνεχίσει να εργάζεται με τον υπολογιστή. Στη συνέχεια για να παράξει τον τυχαίο αριθμό συλλέγει στα 5 αυτά λεπτά τυχαία δεδομένα που εξαρτώνται από τη συμπεριφορά του χρήστη (κινήσεις ποντικιού, πλήκτρα του πληκτρολογίου που πατήθηκαν, κύκλοι μηχανής που καταναλώθηκαν κοκ). Με βάση αυτά τα πραγματικά τυχαία δεδομένα υπολογίζεται ο τυχαίος αριθμός και εισάγεται στη γεννήτρια κλειδιών για να κατασκευαστεί το δημόσιο και το ιδιωτικό κλειδί του χρήστη.

3.2.2 Εμπιστευτικότητα

Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού μπορούν να εγγυηθούν εμπιστευτικότητα (confidentiality), δηλαδή ότι το κρυπτογραφημένο μήνυμα που θα στείλει ο αποστολέας μέσω του διαδικτύου στον παραλήπτη θα είναι αναγνώσιμο από αυτόν και μόνο. Για να επιτευχθεί η εμπιστευτικότητα, ο αποστολέας θα πρέπει να χρησιμοποιήσει το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα. Στη συνέχεια στέλνει το κρυπτογραφημένο μήνυμα στον παραλήπτη και ο τελευταίος μπορεί να το αποκρυπτογραφήσει με το ιδιωτικό κλειδί του. Δεδομένου ότι το ιδιωτικό κλειδί του παραλήπτη είναι γνωστό μονάχα στον ίδιο και σε κανέναν άλλον, μονάχα ο παραλήπτης μπορεί να αποκρυπτογραφήσει το μήνυμα και να το διαβάσει. Άρα λοιπόν με αυτόν τον τρόπο ο αποστολέας γνωρίζει ότι το κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μονάχα από τον παραλήπτη και έτσι διασφαλίζεται η εμπιστευτικότητα του μηνύματος.



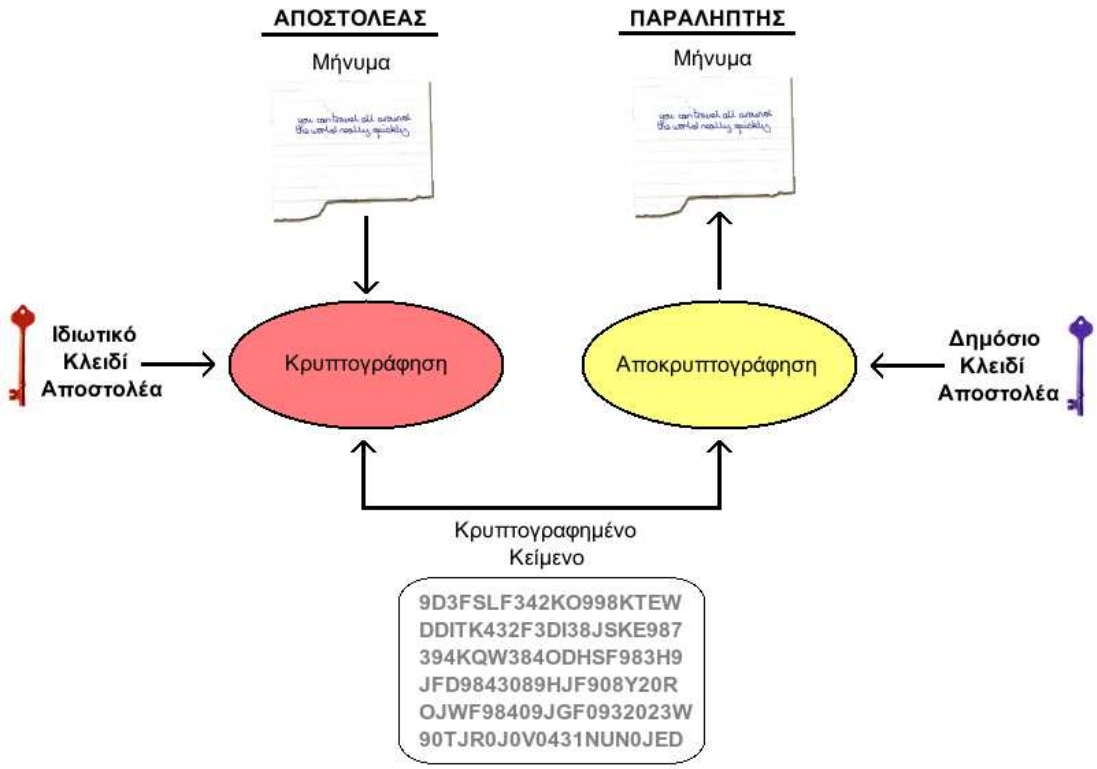
Επίτευξη εμπιστευτικότητας αλλά όχι πιστοποίησης χρησιμοποιώντας κρυπτογραφικούς αλγόριθμους δημοσίου κλειδιού

Η παραπάνω μέθοδος μπορεί να εξασφαλίσει την εμπιστευτικότητα αλλά όχι την πιστοποίηση του αποστολέα. Αυτό με λίγα λόγια σημαίνει πως η παραπάνω μέθοδος δεν μπορεί να εγγυηθεί την ταυτότητα του αποστολέα. Πράγματι, ο αποστολέας μπορεί να δηλώσει ψευδή ταυτότητα και ο παραλήπτης να νομίσει ότι το συγκεκριμένο μήνυμα προήλθε από άλλο πρόσωπο.

3.2.3 Πιστοποίηση

Χρησιμοποιώντας κατάλληλα τους κρυπτογραφικούς αλγορίθμους δημοσίου κλειδιού μπορεί να επιτευχθεί πιστοποίηση (authentication), δηλαδή ο παραλήπτης να γνωρίζει με ασφάλεια την ταυτότητα του αποστολέα. Για να επιτευχθεί αυτό θα πρέπει ο αποστολέας να χρησιμοποιήσει το ιδιωτικό του κλειδί για την κρυπτογράφηση του μηνύματος. Στη συνέχεια στέλνει το μήνυμα στον παραλήπτη και ο τελευταίος χρησιμοποιεί το δημόσιο κλειδί του αποστολέα για την αποκρυπτογράφησή του.

Δεδομένου ότι το ιδιωτικό κλειδί του αποστολέα είναι γνωστό μονάχα στον ίδιο, ο παραλήπτης μπορεί να είναι σίγουρος για την ταυτότητα του αποστολέα.



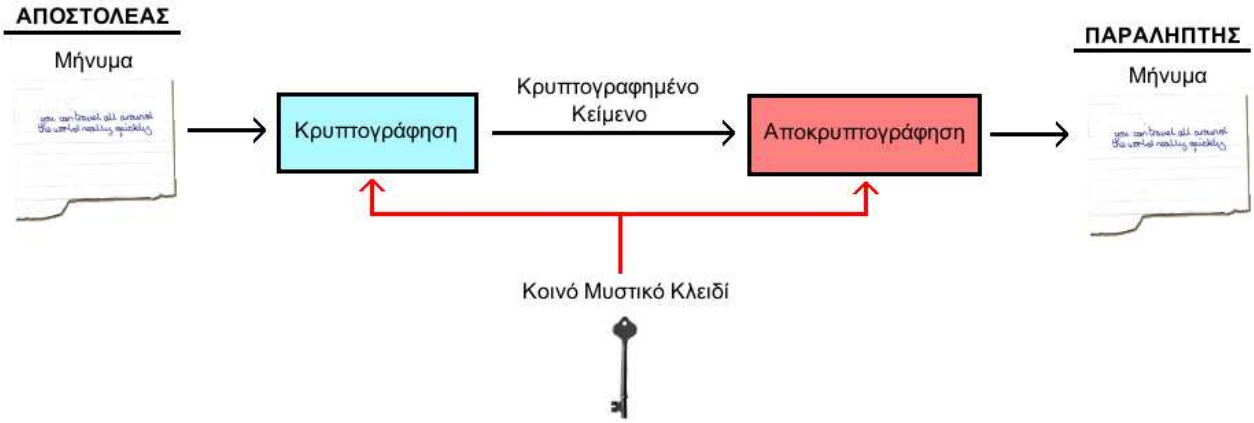
Επίτευξη αυθεντικοποίησης αλλά όχι εμπιστευτικότητας χρησιμοποιώντας κρυπτογραφικούς αλγόριθμους δημοσίου κλειδιού

Παρόλο που η παραπάνω μέθοδος εγγυάται την ταυτοποίηση του αποστολέα, δεν δύναται να εγγυηθεί την εμπιστευτικότητα του μηνύματος. Πράγματι, το μήνυμα μπορεί να το αποκρυπτογραφήσει οποιοσδήποτε διαθέτει το δημόσιο κλειδί του αποστολέα. Όπως έχει ήδη ειπωθεί, το δημόσιο κλειδί είναι γνωστό σε όλη τη διαδικτυακή κοινότητα, άρα πρακτικά ο οποιοσδήποτε μπορεί να διαβάσει το περιεχόμενο του μηνύματος.

3.3 Κρυπτογράφηση Συμμετρικού Κλειδιού

Η **κρυπτογράφηση συμμετρικού κλειδιού (Symmetric Cryptography)** βασίζεται στην ύπαρξη ενός και μόνο κλειδιού, το οποίο χρησιμοποιείται τόσο στην κρυπτογράφηση όσο και στην αποκρυπτογράφηση του μηνύματος. Το κλειδί αυτό θα πρέπει να είναι γνωστό μόνο στα συναλλασσόμενα μέρη. Η διαδικασία της

κρυπτογράφησης και αποκρυπτογράφησης φαίνεται πιο παραστατικά στο σχήμα που ακολουθεί:



Η διαδικασία κρυπτογράφησης συμμετρικού κλειδιού

Ένα πρόβλημα το οποίο υφίσταται στους αλγόριθμους κρυπτογράφησης είναι η αδυναμία ανταλλαγής του κλειδιού με κάποιο ασφαλή τρόπο. Στην σύγχρονη ψηφιακή εποχή ο αποστολέας και ο παραλήπτης του μηνύματος πολλές φορές δεν γνωρίζονται, οπότε για την μετάδοση του κλειδιού από τον έναν στον άλλο θα πρέπει να υπάρχει κάποιο ασφαλές κανάλι επικοινωνίας. Φυσικά το διαδίκτυο δεν μπορεί να αποτελέσει κανάλι ασφαλούς επικοινωνίας, οπότε η χρήση της συμμετρικής κρυπτογράφησης σε εφαρμογές ηλεκτρονικού εμπορίου, ανταλλαγής ηλεκτρονικών μηνυμάτων κοκ ουσιαστικά δεν υφίσταται.

Το βασικό πλεονέκτημα των αλγορίθμων συμμετρικού κλειδιού είναι ότι η διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης είναι πολύ γρήγορη και δεν καταναλώνει σημαντική υπολογιστική ισχύ.

Οι πιο γνωστοί αλγόριθμοι αυτού του είδους είναι οι DES, Triple DES, IDEA, RC2, RC4, AES.

3.4 Αλγόριθμοι Ασύμμετρης Κρυπτογραφίας

RSA

Το σύστημα RSA είναι ένα σύστημα ασύμμετρης κρυπτογραφίας που προσφέρει Τεχνικές κρυπτογράφησης και ψηφιακές υπογραφές. Αναπτύχθηκε το 1977 από

τους Ron Rivest, Adi Shamir και Leonard Adleman. Από τα αρχικά των επιθέτων τους προέρχεται το ακρωνύμιο RSA.

Το RSA λειτουργεί ως εξής: παίρνουμε δύο μεγάλους πρώτους αριθμούς *p,q* και υπολογίζουμε το γινόμενο τους $n = pq$. Το *n* καλείται *modulus*. Διαλέγουμε ένα αριθμό *e* μικρότερο του *n* και τέτοιο, ώστε *e* και $(p-1)(q-1)$ να μην έχουν κοινούς διαιρέτες εκτός του 1. Βρίσκουμε έναν άλλο αριθμό *d*, ώστε $(ed-1)$ να διαιρείται από το $(p-1)(q-1)$. Τα ζευγάρια (n,e) και (n,d) καλούνται δημόσια κλείδα και ιδιωτική κλείδα, αντίστοιχα.

Είναι δύσκολο να βρεθεί η ιδιωτική κλείδα *d* από την δημόσια κλείδα *e*. Αυτό θα απαιτούσε την εύρεση των διαιρετέων του πρώτου αριθμού *n*, δηλαδή των αριθμών *p* και *q*. Ο *n* είναι πολύ μεγάλος και επειδή είναι πρώτος, θα έχει μόνο δύο πρώτους διαιρέτες. Άρα η εύρεση των διαιρετέων είναι πολύ δύσκολη έως και αδύνατη. Στο άλυτο αυτού του προβλήματος βασίζεται το σύστημα RSA. Η ανακάλυψη μιας εύκολης μεθόδου επίλυσης του προβλήματος θα αχρήστευε το RSA.

Με το RSA η κρυπτογράφηση και η πιστοποίηση ταυτότητας πραγματοποιούνται χωρίς των κοινή χρήση ιδιωτικών κλείδων. Ο καθένας χρησιμοποιεί μόνο την δικιά του ιδιωτική κλείδα ή την δημόσια κλείδα οποιουδήποτε αλλού. Όλοι μπορούν να στείλουν ένα κρυπτογραφημένο μήνυμα ή να επαληθεύσουν μια υπογραφή, αλλά μόνο ο κάτοχος της σωστής ιδιωτικής κλείδας μπορεί να αποκρυπτογραφήσει ή να υπογράψει ένα μήνυμα.

Κρυπτογράφηση με το RSA

Έστω ο χρήστης Α που θέλει να στείλει ένα κρυπτογραφημένο έγγραφο στον χρήστη Β. Ο Α κρυπτογραφεί το έγγραφο με την εξής εξίσωση: $c = m^e \bmod n$,
όπου (n,e) είναι η δημόσια κλείδα του Β. Ο Β, όταν παραλάβει το μήνυμα θα εφαρμόσει την εξής εξίσωση: $m = c^d \bmod n$, όπου (n,d) η ιδιωτική κλείδα του Β. Η μαθηματική σχέση που το *e* και το *d* εξασφαλίζει το γεγονός ότι ο Β αποκρυπτογραφεί το μήνυμα. Αφού μόνο ο Β ξέρει το *d*, μόνο αυτός μπορεί να αποκρυπτογραφήσει το μήνυμα.

Ψηφιακές Υπογραφές με το RSA

Ας υποθέσουμε, τώρα, ότι ο Α θέλει να στείλει μήνυμα στον Β με τέτοιον τρόπο ώστε ο Β να είναι σίγουρος ότι το μήνυμα είναι αυθεντικό και δεν έχει μεταβληθεί. Ο Α υπογράφει το έγγραφο ως εξής: $s = m^d \ mod \ n$, όπου d και n είναι η ιδιωτική κλείδα του Α. Για να επαληθεύσει την υπογραφή ο Β εκτελεί την πράξη: $m = s^e \ mod \ n$, όπου e και n η δημόσια κλείδα του Α.

3.5 Αλγόριθμοι Συμμετρικής Κρυπτογραφίας

DES (Data Encryption Standard)

DES είναι το ακρωνύμιο των λέξεων ***D**ata **E**ncryption **S**tandard*. Αντιπροσωπεύει την τυποποίηση *Federal Information Processing Standard (FIPS)* 46-1 που επίσης περιγράφει τον *Data Encryption Algorithm (DEA)*. Αρχικά αναπτύχθηκε από την IBM, ενώ σημαντικό ρόλο στην ανάπτυξη του έπαιξε η NSA και το *National Institute of Standards and Technology (NIST)*. Είναι ο πιο γνωστός και παγκόσμια χρησιμοποιούμενος συμμετρικός αλγόριθμος.

Ο DES είναι block cipher, πιο συγκεκριμένα Feistel cipher, με μέγεθος block 64 bit. Χρησιμοποιεί κλειδί 64 bits από τα οποία τα 8 αποτελούν bits ισοτιμίας. Όταν χρησιμοποιείται για την επικοινωνία, αποστολέας και παραλήπτης μοιράζονται το ίδιο κλειδί. Ο DES, εκτός από κρυπτογράφηση, μπορεί να χρησιμοποιηθεί στην παραγωγή MACs (σε CBC mode). Επίσης, μπορεί να χρησιμοποιηθεί για κρυπτογράφηση αρχείων αποθηκευμένα σε σκληρό δίσκο σε περιβάλλοντα ενός χρήστη. Για την διανομή των κλειδιών σε περιβάλλον πολλών χρηστών, συνδυάζεται με ασύμμετρο κρυπτοσύστημα.

Triple-DES

Είναι μια παραλλαγή του DES όπου το μήνυμα κρυπτογραφείται και αποκρυπτογραφείται διαδοχικά με διαφορετικά κλειδιά για την ενίσχυση του βασικού αλγόριθμου. Υπάρχουν τέσσερις διαφορετικοί τρόποι για να επιτευχθεί αυτό:

- DES-EEE3 *(Encrypt-Encrypt-Encrypt)*: πραγματοποιούνται τρεις συνεχόμενες κρυπτογραφήσεις με τα τρία διαφορετικά κλειδιά.
- DES-EDE3 *(Encrypt-Decrypt-Encrypt)*: το μήνυμα διαδοχικά κρυπτογραφείται, αποκρυπτογραφείται και τέλος κρυπτογραφείται με χρήση τριών διαφορετικών κλειδιών.
- DES-EEE2: είναι η ίδια με την πρώτη διαδικασία εκτός του ότι απαιτούνται δύο διαφορετικά κλειδιά.
- DES-EDE2: είναι η ίδια με την δεύτερη διαδικασία εκτός του ότι απαιτούνται δύο κλειδιά.

Τα επιπλέον κλειδιά δημιουργούνται από το κοινό μυστικό κλειδί με κατάλληλο αλγόριθμο. Από αυτούς τους τρόπους, ο πιο ασφαλής είναι ο DES-EEE3, με την τριπλή κρυπτογράφηση και τα τρία διαφορετικά κλειδιά.

DESX

Ο DESX είναι μια άλλη παραλλαγή του DES. Η διαφορά του DES και του DESX είναι ότι η είσοδος στο DESX περνάει από μια X-OR πράξη με ένα επιπλέον κλειδί 64 bits και ομοίως η έξοδος της κρυπτογράφησης. Η αιτία ανάπτυξης του DESX είναι η δραματική αύξηση της αντοχής του DES σε γνωστές επιθέσεις.

AES (Advanced Encryption Standard)

Το ακρωνύμιο AES προέρχεται από την φράση *Advanced Encryption Standard*. Είναι ένας block cipher που προορίζεται να γίνει τυποποίηση του FIPS και να αντικαταστήσει τον DES. Ο DES βρίσκεται ήδη πολλά χρόνια σε χρήση και από το 1998 το NIST δεν τον ανανεώνει.

DSS (Digital Signature Algorithm)

Το National Institute of Standards and Technology (NIST) δημοσιοποίησε το *Digital Signature Algorithm (DSS)*, που είναι μέρος του *Capstone Project* της κυβέρνησης των Ηνωμένων Πολιτειών, τον Μάιο του 1994. Έχει καθιερωθεί σαν το επίσημο αλγόριθμο παραγωγής ψηφιακών υπογραφών της κυβέρνησης των Η.Π.Α.

Βασίζεται στο πρόβλημα του διακριτού λογαρίθμου και χρησιμοποιείται μόνο για παραγωγή ψηφιακών υπογραφών. Η διαφορά από τις υπογραφές του RSA είναι ότι ενώ στο DSA η παραγωγή των υπογραφών είναι πιο γρήγορη από την επιβεβαίωση τους, στο RSA συμβαίνει το αντίθετο: η επιβεβαίωση είναι ταχύτερη από την υπογραφή. Παρ' όλο που μπορεί να υποστηριχθεί ότι η γρήγορη παραγωγή υπογραφών αποτελεί πλεονέκτημα, επειδή ένα μήνυμα υπογράφεται μία φορά αλλά η υπογραφή του μπορεί να επαληθευτεί πολλές φορές, κάτι τέτοιο δεν ανταποκρίνεται στην πραγματικότητα.

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

RC2, RC4, RC5

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

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

Ο **RC5** είναι ένας γρήγορος block cipher από τον Ron Rivest για λογαριασμό της RSA Inc το 1994. Έχει πολλούς παραμέτρους: μεταβλητό μήκος κλειδιού, μεταβλητό μέγεθος block και μεταβλητό αριθμό επαναλήψεων. Τυπικές επιλογές για το μέγεθος του block είναι 32 bits (για πειραματικές εφαρμογές), 64 bits (για αντικατάσταση του DES) και 128 bits. Ο αριθμός των επαναλήψεων μπορεί να είναι

από 0 έως και 255. Ο RC5 είναι πολύ απλός στην λειτουργία, πράγμα που τον κάνει εύκολο στην ανάλυση.

IDEA (International Data Encryption Algorithm)

Ο IDEA είναι ένας block cipher που αναπτύχθηκε από
τους Lai και Massey. Χρησιμοποιεί block μεγέθους 64 bits και κλειδιά 128 bits. Η διαδικασία της κρυπτογράφησης απαιτεί 8 σύνθετες επαναλήψεις. Παρ' όλο που δεν έχει την κατασκευή ενός Feistel cipher, η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο που γίνεται και η κρυπτογράφηση. Έχει σχεδιαστεί για να είναι εύκολα εφαρμόσιμος τόσο hardware σε όσο και σε software. Μερικές, όμως, αριθμητικές διεργασίες που χρησιμοποιεί ο IDEA καθιστούν τις λογισμικές εφαρμογές αργές, παρόμοιες σε ταχύτητα με τον DES. Ο IDEA αποτελεί ένα πολύ δυνατό αλγόριθμο που είναι απρόσβλητος από τα περισσότερα είδη επιθέσεων.

Κεφάλαιο 4^{ο} : Φράγματα ασφαλείας (firewalls)

4.1 Ορισμός των Φραγμάτων Ασφάλειας

Φράγμα ασφάλειας ονομάζεται ένα σύστημα που αποτελείται από δικτυακά στοιχεία τα οποία τοποθετούνται μεταξύ δύο δικτύων και το οποίο έχει τα ακόλουθα χαρακτηριστικά:

1. Όλη η δικτυακή κίνηση από και προς το εσωτερικό δίκτυο πρέπει να περάσει μέσα από αυτό το σύστημα.
2. Η διέλευση επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες, όπως αυτή καθορίζεται από την τοπική πολιτική ασφάλειας.
3. Είναι αδιαπέραστο σε απόπειρες διείσδυσης.

Ο όρος «φράγμα ασφαλείας» αναφέρεται σε οποιοδήποτε συνδυασμό στοιχείων υλικού, λογισμικού και πολιτικής ασφάλειας που τοποθετείται μεταξύ ενός ιδιωτικού (συνήθως ένα ενδοεπιχειρησιακό δίκτυο) και ενός εξωτερικού δικτύου (συνήθως το Διαδίκτυο). Ως τέτοιο, το φράγμα ασφάλειας υλοποιεί κάποια μέρη της λεγόμενης Πολιτικής Ασφαλείας Δικτύου (NSP-**N**etwork **S**ecurity **P**olicy) με το να αναγκάζει όλη την κίνηση δεδομένων να κατευθυνθεί ή να δρομολογηθεί προς αυτό, όπου μπορεί να εξετασθεί και να αποφασιστεί αν θα επιτραπεί η διέλευσή της. Δηλαδή, το φράγμα ασφαλείας προσπαθεί να αποτρέψει την ανεπιθύμητη και μη εξουσιοδοτημένη επικοινωνία από και προς το ενδοεπιχειρησιακό δίκτυο (intranet) καθώς και να επιτρέψει στον οργανισμό να επιβάλλει μια πολιτική ασφάλειας σχετικά με τη ροή των δεδομένων μεταξύ του ιδιόκτητου δικτύου και του Διαδικτύου.

4.2 Η Αναγκαιότητα Χρήσης των Φραγμάτων Ασφάλειας

Χωρίς την ύπαρξη φράγματος ασφάλειας, ένας δικτυακός τόπος κινδυνεύει από ανασφαλή λειτουργικά συστήματα, υπηρεσίες και πρωτόκολλα, και κατά συνέπεια εκτίθεται σε επιθέσεις εισβολέων. Σε ένα περιβάλλον χωρίς φράγματα ασφάλειας η δικτυακή ασφάλεια αποτελεί αποκλειστικά μέριμνα του κάθε σταθμού ξεχωριστά και όλοι οι σταθμοί θα πρέπει κατά κάποιον τρόπο να συνεργάζονται ώστε να παρέχουν ένα ομοιόμορφα υψηλό επίπεδο ασφάλειας.

Επίσης, όσο πιο μεγάλο είναι το δίκτυο, τόσο πιο δύσκολα επιτυγχάνεται η διατήρηση όλων των σταθμών σε υψηλά επίπεδα ασφάλειας. Και όσο τα λάθη και οι παραλήψεις στην ασφάλεια γίνονται όλο και πιο συχνά, εξαιτίας κυρίως της πολυπλοκότητας του δικτύου, τόσο περισσότερες διεισδύσεις μπορούν να σημειωθούν όχι μόνο ως αποτέλεσμα αλλά μελετημένων επιθέσεων, αλλά και ως αποτέλεσμα λαθών στις ρυθμίσεις διαφόρων αρχείων και στην ανεπιτυχή επιλογή κωδικών πρόσβασης. Δεδομένου ότι το λογισμικό έχει συνήθως σφάλματα, μπορεί κάποιος να ισχυριστεί ότι τα περισσότερα συστήματα υπολογιστών έχουν «οπές» ασφάλειας τις οποίες μπορούν να ανακαλύψουν και να εκμεταλλευτούν οι εισβολείς. Τα φράγματα ασφάλειας έχουν σχεδιαστεί έτσι ώστε να έχουν προηγμένες λειτουργίες παρακολούθησης και καταγραφής και η διαχείρισή τους να είναι σχετικά εύκολη.

Όμως, όπως έχει ήδη αναφερθεί, τα φράγματα ασφάλειας δεν αποτελούν την πανάκεια για όλα τα θέματα ασφάλειας. Ίσως ένα από τα κύρια μειονεκτήματα των φραγμάτων ασφαλείας είναι ότι δεν μπορούν να προστατεύσουν δικτυακούς τόπους και ενδοεπιχειρησιακά δίκτυα (intranets) από επιθέσεις που προέρχονται εκ των έσω. Αν υπάρχει τέτοιο πρόβλημα, θα πρέπει να χρησιμοποιούνται εσωτερικά φράγματα ασφάλειας για να ελέγχουν την πρόσβαση μεταξύ διαφορετικών τμημάτων της εταιρίας ή για να προστατεύουν τα ευαίσθητα μέρη του ενδοεπιχειρησιακού δικτύου. Τα εσωτερικά φράγματα ασφαλείας καλούνται «φράγματα ασφάλειας ενδοεπιχειρησιακού δικτύου» (intranet firewalls).Από καθαρά τεχνική άποψη, δεν υπάρχει τίποτα που να διακρίνει ένα φράγμα ασφάλειας ενδοεπιχειρησιακού δικτύου από ένα φράγμα ασφάλειας Διαδικτύου (Internet firewalls) πέραν της πολιτικής ασφάλειας που αυτό εφαρμόζει.

4.3 Φίλτρα Πακέτων

1η γενιά - Φίλτρα πακέτων

Το πρώτο ερευνητικό δημοσίευμα πάνω στην τεχνολογία firewall προέκυψε το 1988 όταν οι μηχανικοί της DEC (Digital Equipment Corporation) ανέπτυξαν φίλτρα πακέτων δεδομένων (data packet filters). Τα φίλτρα αυτά θεωρούνται ως η πρώτη γενιά firewall.

Τα φίλτρα πακέτων δρουν ως εξής: Διαβάζουν τα πακέτα δεδομένων που διακινούνται από το ένα δίκτυο στο άλλο και, εάν κάποιο πακέτο ταιριάζει με κάποιο συγκεκριμένο κανόνα, τότε το απορρίπτουν. Ο διαχειριστής του δικτύου είναι σε θέση να ορίσει τους κανόνες βάσει των οποίων θα απορρίπτονται τα πακέτα. Αυτός ο τύπος firewall δεν ενδιαφέρεται για το εάν κάποιο πακέτο ανήκει σε μία σύνδεση, δηλαδή δεν αποθηκεύει πληροφορίες σχετικά με την κατάσταση των διαφόρων συνδέσεων από το ένα δίκτυο στο άλλο (stateless packet filtering). Αντιθέτως, φιλτράρει κάθε πακέτο με βάση την πληροφορία που περιέχεται στο ίδιο το πακέτο (π.χ. διεύθυνση IP προέλευσης, διεύθυνση IP προορισμού, πρωτόκολλο, αριθμός θύρας κοκ). Επειδή τα πρωτόκολλα TCP και UDP χρησιμοποιούν τις ευρέως διαδεδομένες θύρες (Well known ports), ένα firewall πρώτης γενιάς μπορεί να ξεχωρίσει τα πακέτα που αφορούν διάφορες λειτουργίες, όπως για παράδειγμα το email, την μεταφορά αρχείων, την περιήγηση στο Διαδίκτυο κοκ.

2η γενιά - Φίλτρα κατάστασης

Η δεύτερη γενιά firewall αναπτύχθηκε από τρεις ερευνητές στα εργαστήρια της AT&T Bell: Dave Presetto, Howard Trickey και Kshitij Nigam.

Τα firewall της δεύτερης γενιάς δρουν όπως τα firewall πρώτης γενιάς με κάποιες επιπρόσθετες λειτουργίες. Μία από αυτές είναι το γεγονός ότι πλέον εξετάζουν και την κατάσταση (state) του κάθε πακέτου, δηλαδή την σύνδεση από την οποία προήλθε. Για τον λόγο αυτό και αναφέρονται ως φίλτρα κατάστασης (stateful firewalls). Τα φίλτρα αυτά κρατούν ανά πάσα στιγμή πληροφορίες για τον αριθμό και το είδος των συνδέσεων μεταξύ των δύο δικτύων και επιπλέον μπορούν να ξεχωρίσουν εάν ένα πακέτο αποτελεί την αρχή ή το τέλος μία νέας σύνδεσης ή μέρος μίας ήδη υπάρχουσας.

Οι διαχειριστές τέτοιων firewalls μπορούν να ορίσουν τους κανόνες βάσει των οποίων θα επιτρέπεται η δημιουργία συνδέσεων από το εξωτερικό δίκτυο (Διαδίκτυο) προς το τοπικό/εταιρικό δίκτυο. Με τον τρόπο αυτό γίνεται πιο εύκολη η πρόληψη διαφόρων ειδών επιθέσεων, όπως για παράδειγμα ή επίθεση SYN flood.

3η γενιά - Επίπεδο εφαρμογών

Η τρίτη γενιά firewall βασίζεται πλέον στο επίπεδο εφαρμογών σύμφωνα με το μοντέλο αναφοράς OSI (Open Systems Interconnection). Το κύριο χαρακτηριστικό αυτής της γενιάς firewall είναι ότι μπορεί να αντιλαμβάνεται ποια προγράμματα και

πρωτόκολλα προσπαθούν να δημιουργήσουν μία νέα σύνδεση (πχ FTP - File Transfer Protocol, DNS - Domain Name System, περιήγηση στο Διαδίκτυο κοκ). Με τον τρόπο αυτό μπορούν να εντοπιστούν εφαρμογές που προσπαθούν να δημιουργήσουν ανεπιθύμητες συνδέσεις ή καταχρήσεις ενός πρωτοκόλλου ή μιας υπηρεσίας.

Σήμερα

Σήμερα σιγά σιγά εδραιώνονται τα firewalls 4ης γενιάς, τα οποία διαθέτουν γραφικό περιβάλλον μέσω του οποίου μπορεί ο χρήστης να κάνει τις επιλογές του όσον αφορά την ασφάλεια του δικτύου του και να θέσει τους κανόνες βάσει τον οποίων θα απορρίπτονται κάποια πακέτα ή συνδέσεις. Τα firewalls 4ης γενιάς μπορούν πλέον να ενσωματωθούν στο λειτουργικό σύστημα και συνεργάζονται στενά με άλλα συστήματα ασφαλείας, όπως για παράδειγμα το IPS - Intrusion Prevention System.

Πολιτικές Firewall

Οι «πολιτικές» για τα «τείχη προστασίας» (Firewall policies) υπαγορεύουν τις διαδικασίες χειρισμού της κυκλοφορίας στα υπολογιστικά δίκτυα (computer networks) για συγκεκριμένες «IP – Internet Protocol» διευθύνσεις και το εύρος αυτών, για τα πρωτόκολλα, τις εφαρμογές και τους τύπους ενεργού περιεχομένου, βασισμένες στις πολιτικές ασφαλείας (security policies) των πληροφοριών κάθε οργανισμού. Η ανάλυση των πιθανών κινδύνων και η ανάπτυξη ενός καταλόγου ο οποίος θα περιλαμβάνει λίστα με τα δεδομένα που διακινούνται εντός του δικτύου, θα πρέπει να προηγείται οποιασδήποτε άλλης διαδικασίας. Η οργάνωση και η κατηγοριοποίηση των δεδομένων διασφαλίζει εν μέρει την ακεραιότητα των δεδομένων τα οποία διασχίζουν το τείχος προστασίας . Η επιτυχής υλοποίηση της παραπάνω διαδικασίας επιτρέπει την υλοποίηση πολιτικών για τα τείχη προστασίας (Firewall Policies).

Η εν λόγω ανάλυση κινδύνου (risk analysis) θα πρέπει να βασίζεται στην αξιολόγηση των πιθανών απειλών , των τρωτών σημείων και των επιπτώσεων για τα δεδομένα ή τα υπολογιστικά συστήματα σε περίπτωση κινδύνου. Επιπλέον κρίνεται αναγκαία η τεκμηρίωση των πολιτικών για τα τείχη προστασίας και η συχνή ενημέρωση αυτών για νέες μορφές επιθέσεων ή τρωτά σημεία βάσει των αναγκών του οργανισμού.

4.4 Πύλες Εφαρμογών (Application Gateways)

Τα gateways επιπέδου εφαρμογής ή application gateways προγραμματίζονται ώστε να καταλαβαίνουν την κίνηση στο επίπεδο εφαρμογής του TCP/IP. Έτσι, παρέχουν ελέγχους προσπέλασης σε επίπεδο χρήστη και σε επίπεδο πρωτοκόλλων εφαρμογής. Τα application gateways υιοθετήθηκαν προκειμένου να εξαλειφθούν κάποιες από τις αδυναμίες που εμφανίστηκαν στην υλοποίηση των φίλτρων στους δρομολογητές. Έτσι, χρησιμοποιούνται software εφαρμογές, οι οποίες προωθούν και φιλτράρουν συνδέσεις για υπηρεσίες όπως HTTP, TELNET και FTP. Μια τέτοια εφαρμογή καλείται proxy υπηρεσία. Ένας χρήστης που επιθυμεί να συνδεθεί στο σύστημα, θα πρέπει πρώτα να συνδεθεί στο gateway και ύστερα στο host προορισμού, όπως και στο παράδειγμα που ακολουθεί :

1) Ο χρήστης κάνει telnet στο application gateway και πληκτρολογεί το όνομα ενός εσωτερικού host,

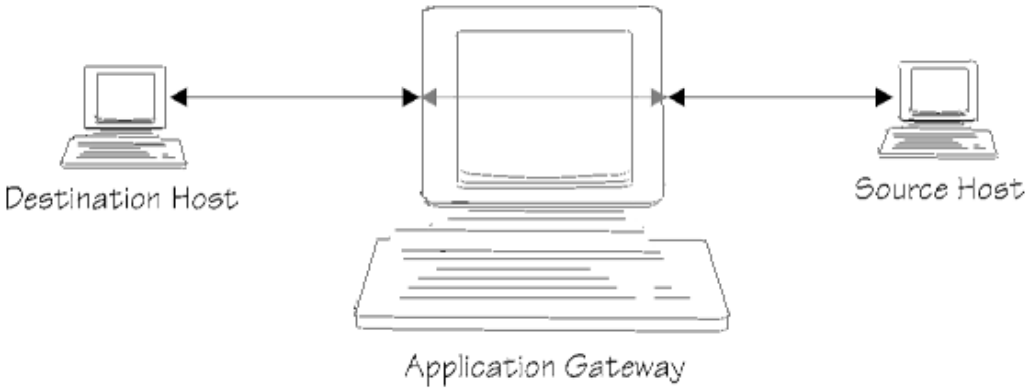
2) Το gateway ελέγχει την IP διεύθυνση του χρήστη (source) και την εγκρίνει ή την απορρίπτει, σύμφωνα με ορισμένα κριτήρια προσπέλασης,

3) Ο χρήστης ενδεχομένως να πρέπει να αυθεντικοποιήσει τον εαυτό του (π.χ χρησιμοποιώντας μια one-time password συσκευή),

4) Η proxy υπηρεσία δημιουργεί μια TELNET σύνδεση μεταξύ του gateway και του εσωτερικού host,

5) Η proxy υπηρεσία “μεταφέρει” bytes μεταξύ των δύο συνδέσεων, και

6) Το application gateway καταγράφει (log) τη σύνδεση.



Virtual (εικονική) Σύνδεση που υλοποιείται από το application gateway και τις proxy

“Πώς δουλεύει”

Το Gateway έχει την ευθύνη να λαμβάνει πακέτα από το ένα δίκτυο και να τα παραδίδει σε ένα άλλο δίκτυο. Συνήθως αυτό σημαίνει ότι λαμβάνει πακέτα από το Internet και τα παραδίδει στο τοπικό δίκτυο (και αντιστρόφως). Το Gateway “ανοίγει” τα πακέτα, εξετάζει το περιεχόμενό τους, και εξασφαλίζει ότι δεν μπορούν να βλάψουν δυνητικά το τοπικό δίκτυο. Αφού τα πακέτα ελέγχονται ως προς την ασφάλειά τους, το Gateway “χτίζει” καινούρια, με το ίδιο περιεχόμενο. Έτσι, μόνο οι τύποι πακέτων για τους οποίους υπάρχει κώδικας κατασκευής μπορούν να εγκαταλείψουν το Gateway. Είναι αδύνατον να σταλεί μη εξουσιοδοτημένος τύπος πακέτου, αφού δεν υπάρχει κώδικας για να το δημιουργήσει. Έτσι αποτρέπονται τα “back doors”. Τα καινούρια πακέτα στέλνονται μέσω ενός ξεχωριστού interface δικτύου.

Για να χρησιμοποιήσουν το Gateway, οι χρήστες πρέπει να συνδεθούν (log in) με την Gateway μηχανή, ή να υλοποιήσουν μια συγκεκριμένη client εφαρμογή σε κάθε host από τον οποίο θα συνδεθούν. Έτσι, ένα custom πρόγραμμα πρέπει να γραφτεί για κάθε εφαρμογή, και οι εφαρμογές που επιτρέπονται είναι μονάχα αυτές για τις οποίες έχει γραφτεί πρόγραμμα. Αυτό ίσως να είναι ένα εγγενές μειονέκτημα, αλλά αποτελεί πλεονέκτημα ως προς την ασφάλεια του συστήματος, καθώς εφαρμόζει πλήρως την φιλοσοφία “Αυτό που δεν επιτρέπεται ρητά, απαγορεύεται”.

Το custom πρόγραμμα εφαρμογής λειτουργεί ως proxy που δέχεται κλήσεις και τις εξετάζει με βάση λίστες προσπέλασης που διαθέτει. Στην περίπτωση αυτή το proxy λειτουργεί ως proxy server. Λαμβάνοντας την κλήση και αφότου πιστοποιηθεί ότι η κλήση είναι επιτρεπόμενη, ο proxy προωθεί την αίτηση στον αντίστοιχο server. Τότε, ο proxy λειτουργεί τόσο ως server, όσο και ως client. Ως server προκειμένου να λάβει την αίτηση και ως client προκειμένου να την προωθήσει. Αφότου εγκατασταθεί η σύνδεση (session), ο proxy απλά αντιγράφει και μεταδίδει τα δεδομένα ανάμεσα στον client που έκανε την αίτηση και στον server τον οποίο στόχευε η αίτηση.

Εφόσον είναι απαραίτητη μια custom client εφαρμογή για την επικοινωνία με τον proxy server, ορισμένες standard κλήσεις συστήματος, όπως η connect( ), πρέπει να αντικατασταθούν με μια proxy έκδοση αυτών των κλήσεων συστήματος. Έπειτα, η client εφαρμογή πρέπει να μεταγλωττιστεί και να συνδεθεί με τις proxy αυτές εκδόσεις. Μία δωρεάν διαθέσιμη βιβλιοθήκη (library), η SOCKS, είναι διαθέσιμη στο URL: ftp://ftp.inoc.dl.nec.com/pub/security/socks.cstc.

Πλεονεκτήματα των Application Gateways

Πλεονεκτήματα από τη χρήση των application gateways για την προστασία του συστήματος μπορούν να θεωρηθούν τα εξής:

• Τα gateways μπορούν να απορρίψουν ή να επιτρέψουν μια σύνδεση, βασιζόμενα όχι μόνο στο όνομα χρήστη, στις διευθύνσεις και τα πρωτόκολλα, αλλά προχωρούν πιο “βαθειά”: μπορούν για παράδειγμα να φιλτράρουν μια FTP σύνδεση, επιτρέποντας τη χρήση της εντολής “get” και απαγορεύοντας τη χρήση της εντολής “put”.

• Μπορούν να φιλτράρουν Java applets και ActiveX προγράμματα.

• Δεν επιτρέπουν την εκτέλεση εφαρμογών για τις οποίες δεν έχει γραφτεί proxy, όπως ήδη αναφέρθηκε, αυξάνοντας την ασφάλεια του συστήματος.

• Αποκρύπτουν πληροφορίες για το σύστημα, αφού τα ονόματα των εσωτερικών hosts δεν είναι απαραίτητο να είναι γνωστά μέσω DNS σε απομακρυσμένα συστήματα. Τα συστήματα αυτά χρειάζεται να γνωρίζουν μόνο το όνομα του host που “φιλοξενεί” το application gateway”.

• Υποστηρίζουν τη δυνατότητα αυθεντικοποίησης (authentication) και καταγραφής (logging).

• Είναι αποτελεσματικά ως προς το κόστος τους, καθώς το ανεξάρτητο software ή hardware που απαιτείται για την αυθεντικοποίηση ή την καταγραφή, εγκαθίσταται μόνο στο application gateway host και πουθενά αλλού.

• **Σε περίπτωση που συνδυάζονται με packet filtering δρομολογητές**, απαιτούν λιγότερο περίπλοκους κανόνες φιλτραρίσματος, από ότι εάν υφίστατο μονάχα ο δρομολογητής. Αυτό συμβαίνει διότι το μόνο που πρέπει να κάνει ο δρομολογητής είναι να επιτρέπει πακέτα που προορίζονται για το application gateway.

4.5 Firewalls: Ολοένα και περισσότερο ασφαλή

Σε πολύ σύντομο χρονικό διάστημα, τα firewalls έχουν κερδίσει την εκτίμηση των περισσότερων οργανισμών στο Internet . Χωρίς αυτά, οι administrators (διαχειριστές) ενός δικτύου θα έπρεπε να διατηρούν την ασφάλεια όλων των συστημάτων τους σε υψηλό επίπεδο, κάτι που είναι εξαιρετικά δύσκολο αν λάβει κανείς υπ'όψιν του το γεγονός ότι ο αριθμός των συστημάτων ανά δίκτυο αυξάνει ραγδαία στις μέρες μας.

Αυξημένες απειλές

Η σημερινή κατάσταση στο Internet εξακολουθεί να είναι πηγή ανησυχιών για τους administrators δικτύων. Ενώ πρέπει να φροντίζουν ώστε οι χρήστες να είναι "ευτυχισμένοι", με την υιοθέτηση νέων υπηρεσιών, ταυτόχρονα πρέπει να μεριμνούν για την ασφάλειά τους. Όμως, καθώς ο αριθμός των χρηστών και των υπηρεσιών αυξάνεται κάθε μέρα, έτσι αυξάνονται και οι διαγραφόμενες απειλές.

Σήμερα υπάρχουν ειδικές ομάδες σύνταξης αναφορών περί παραβιάσεων στο Internet (π.χ η CERT*), οι οποίες δέχονται καθημερινά χιλιάδες κλήσεις από χρήστες που έχουν να αναφέρουν κάποια παραβίαση στο σύστημά τους. Επίσης, τα θέματα περί ασφαλείας έχουν γίνει πλέον αντικείμενο "ανοικτής" συζήτησης σε mailing lists και σε newsgroups στο USENET, όπου συζητούνται και καυτηριάζονται οι αδυναμίες των συστημάτων και οι τρόποι εκμετάλλευσής των. Έτσι, αποτρέπονται αλλά και δημιουργούνται καινούριες παραβιάσεις.

Οι source-route επιθέσεις που στοχεύουν τα συστήματα πίσω από τα firewalls, έχουν γίνει ευκολότερες χάρη στην ύπαρξη εργαλείων που αυτοματοποιούν τη διαδικασία.

Επίσης, έχουν αυξηθεί οι επιθέσεις άρνησης υπηρεσίας (denial of service) οι οποίες δημιουργούν σύγχυση και ελαττώνουν την παραγωγικότητα. Συνήθεις επιθέσεις άρνησης υπηρεσίας περιλαμβάνουν το "πλημμύρισμα" (flooding) των e-mail συνδέσεων ώστε να αποτρέψουν τη χρήση τους, καθώς και την αποστολή ICMP echo πακέτων που κορέζουν τα δίκτυα μπλοκάροντας τις επικοινωνίες. Ορισμένα firewalls παραμένουν ευάλωτα σε αυτού του είδους τις επιθέσεις.

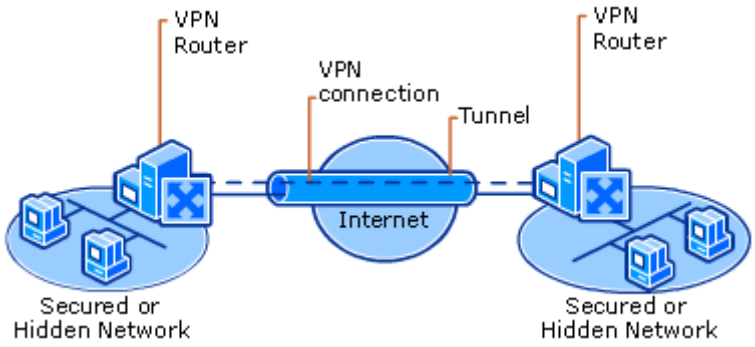
Καινούρια χαρακτηριστικά

Αποκρινόμενοι στις αυξανόμενες απειλές, οι εταιρίες firewalls έχουν εισάγει αρκετά καινούρια χαρακτηριστικά στα προϊόντα τους. Αυτά τα χαρακτηριστικά ποικίλουν από την αύξηση των τύπων των proxies και των υπηρεσιών που υποστηρίζουν, εώς την αύξηση των μηχανισμών ασφαλείας και της ευκολίας διαχείρισης:

• **Εργαλεία Διαχείρισης και Διαμόρφωσης των firewalls** εμφανίζονται καθημερινά στην αγορά του Internet. Ορισμένα firewalls χρησιμοποιούν GUIs (Graphical User Interfaces) ώστε να διευκολύνονται οι administrators στην διαμόρφωσή τους. Άλλα συστήματα firewalls επιτρέπουν την **απομακρυσμένη** άσκηση διαχείρισης και ελέγχου ορθότητας (auditing) μέσω διαφόρων πρωτοκόλλων, όπως το SMTP (Simple mail Transfer Protocol), το SNMP (Simple Network Management Protocol) και το HTTP μέσω του World Wide Web. Εξυπακούεται ότι αυτοί οι μηχανισμοί προϋποθέτουν ισχυρή αυθεντικοποίηση και ελέγχους προσπέλασης.

• **Virtual Private Networks (Εικονικά Ιδιωτικά Δίκτυα)**: Σε πολλές επιχειρήσεις υπάρχει η ανάγκη ασφαλούς επικοινωνίας μεταξύ των ιδιωτικών δικτύων που διαθέτουν σε διαφορετικά σημεία στο Internet. Προκειμένου να εξασφαλίσουν την ασφάλεια τέτοιου είδους επικοινωνιών, οι εταιρίες firewalls εφαρμόζουν κρυπτογραφικούς μηχανισμούς στα προϊόντα τους με σκοπό τη δημιουργία ενός virtual ιδιωτικού δικτύου μεταξύ δύο sites, όπου η πληροφορία μεταδίδεται κρυπτογραφημένη. Τα VPNs επιτυγχάνονται με κρυπτογράφιση στο επίπεδο του Internet Protocol, μεταξύ δύο "συνεργαζόμενων" firewalls. Εφόσον το VPN εγκατασταθεί, οι hosts σε ένα σημείο μπορούν να επικοινωνούν με τους hosts στο απομακρυσμένο σημείο χωρίς το φόβο της παραβίασης της εμπιστευτικότητας των πληροφοριών που ανταλάσσονται. Φυσικά, όπως και σε κάθε κρυπτογραφικό σχήμα,

το VPN είναι ασφαλές εφόσον είναι ασφαλή και τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται.



• **Network Address Translation**:

Σε μια διαδικασία NAT (Μετάφραση Διεύθυνσης Δικτύου), το firewall αντικαθιστά τις IP διευθύνσεις των πακέτων με διαφορετικές διευθύνσεις. Αυτό μπορεί να γίνει για διάφορους λόγους, οι περισσότεροι από τους οποίους σχετίζονται με την ασφάλεια. Καταρχήν, το NAT επιτρέπει σε έναν οργανισμό να αποκρύψει τόσο την ύπαρξη συγκεκριμένων συστημάτων στο εσωτερικό του δίκτυο, όπως και την δομή καθ'αυτή του εσωτερικού του δικτύου. Ένα χαρακτηριστικό που καθιστά το NAT πολύ ελκυστικό αλλά δεν σχετίζεται με την ασφάλεια, είναι η ικανότητά του να μετατρέπει hosts δικτύου με μη μοναδικές διευθύνσεις, σε hosts με μοναδικές διευθύνσεις, επιτρέποντας έτσι στον οργανισμό να συνδεθεί με το Internet.

Αυτή η τεχνική είναι χρήσιμη στο να "κρύβει" διευθύνσεις που περιέχονται σε επικεφαλίδες πακέτων. Εντούτοις, προκειμένου να αποκρύπτονται αποτελεσματικά οι εσωτερικές διευθύνσεις, είναι προτιμότερη η "παρέμβαση" μέσα στο πακέτο καθ'αυτό. Έτσι, ορισμένα προϊόντα firewalls ξαναγράφουν π.χ τις e-mail επικεφαλίδες ώστε να κρύψουν το όνομα του εσωτερικού συστήματος από το οποίο προήλθε το μήνυμα.

• **Καινούρια proxies και υπηρεσίες**:

Με στόχο την επέκταση της λειτουργικότητας των firewalls, ολοένα και περισσότερα proxies προστίθενται στα συστήματα. Αυτό είναι και ένα από τα χαρακτηριστικά στο οποίο “ποντάρουν” οι πωλητές firewalls. Ούτως ή άλλως, εάν δεν υπάρχουν διαθέσιμα τα κατάλληλα proxies, οι υπηρεσίες προς τους πελάτες και τους χρήστες ελαττώνονται αισθητά, ενώ αυξάνεται και ο φόρτος των administrators που πρέπει να παρακάμπτουν τα firewalls διατηρώντας παράλληλα το σύστημα ασφαλές. Κάποια από τα proxies που έχουν ανακοινωθεί είναι:

POP3 - Αυτό το proxy επιτρέπει απομακρυσμένη σύνδεση σε e-mail χωρίς να είναι απαραίτητη η παρουσία ενός SMTP server στον απομακρυσμένο host. Το POP3 πρωτόκολλο υποστηρίζει τη χρήση της εντολής APOP, που επιτρέπει στον απομακρυσμένο client να αυθεντικοποιηθεί στον εσωτερικό POP3 server.

LP (Printer) - Αυτό το proxy επιτρέπει τη διέλευση εργασιών εκτύπωσης (print jobs) μέσω του firewall.

Secure Sockets layer (SSL) και Secure-HTTP (SHTTP)

- Αυτά τα δύο proxies “επεκτείνουν” τα υπάρχοντα HTTP proxies στο να υποστηρίζουν επιπλέον μηχανισμούς ασφαλείας για Web πρόσβαση.

Domain Name System (DNS) - Όταν χρησιμοποιείται το NAT, είτε για να αντιστοιχίσει μη μοναδικές διευθύνσεις σε μοναδικές, είτε για να αποκρύψει εσωτερικές διευθύνσεις, πρέπει να υπάρχει έγκυρη DNS πληροφόρηση τόσο στους εσωτερικούς όσο και στους εξωτερικούς χρήστες. Οι πωλητές firewalls ενσωματώνουν πλέον dual-DNS servers στα προϊόντα τους, ένα για περιορισμένη πληροφόρηση προς το κοινό (το Internet) και ένα για πλήρη πληροφόρηση προς τα εσωτερικά συστήματα του δικτύου.

• **Transparent Proxies** (Διάφανα Proxies): Εκτός από τα proxies που αναφέρθηκαν προηγουμένως, οι πωλητές firewalls υλοποιούν επίσης τα λεγόμενα διαφανα proxies. Διάφανο proxy υφίσταται όταν οι χρήστες δεν ξέρουν ότι όντως χρησιμοποιείται ένα proxy. Οι χρήστες, μπορούν να είναι ενήμεροι για την ύπαρξη ενός proxy, με δύο τρόπους: πρώτον, μερικά proxies απαιτούν αλληλεπίδραση του χρήστη με το firewall,

όπως π.χ η πληκτρολόγηση ενός ID και ενός συνθηματικού. Δεύτερον, ένα μη-διάφανο proxy μπορεί να απαιτεί την εγκατάσταση custom client software από τον χρήστη, όπως π.χ οι clients που βασίζονται στο Socks. Πολλοί οργανισμοί θα προτιμούσαν να μην επιφορτώνουν τους χρήστες τους με τέτοιες διαδικασίες, κάτι που εξασφαλίζεται με τα διάφανα proxies. Εντούτοις, τα διάφανα proxies απαιτούν μερικές ρυθμίσεις σε ορισμένα client sotware. Για παράδειγμα, ένας Web browser πρέπει να υποστεί κάποιες ρυθμίσεις για proxies πρωτοκόλλων όπως το ftp ή το gopher.

• **Καταγραφή (log) και έλεγχος ορθότητας**: Τα περισσότερα firewalls παρέχουν μηχανισμούς καταγραφής (logging) λειτουργιών. Εντούτοις, ορισμένα firewalls παρέχουν τη δυνατότητα υποστήριξης μηχανισμών ελέγχου ορθότητας (audit) και προειδοποιητικών (alert) μηχανισμών. Τα auditing εργαλεία επεξεργάζονται την ήδη καταγραφόμενη (από τα logs) πληροφορία και την παρουσιάζουν με έναν περισσότερο ευανάγνωστο τρόπο. Οι alert μηχανισμοί πληροφορούν σε πραγματικό χρόνο τους administrators για “επικίνδυνες” λειτουργίες που επιχειρούνται στο firewall. Επιπρόσθετα, το SNMP μπορεί να χρησιμοποιηθεί για την **προειδοποίηση** (alert) **απομακρυσμένων hosts.**

Κεφάλαιο 5^{ο} : Ασφάλεια στο Ηλεκτρονικό Εμπόριο

5.1 Ορισμός ηλεκτρονικού εμπορίου

Ως **Ηλεκτρονικό Εμπόριο** (Η.Ε.) ή ευρέως γνωστό ως e-commerce, eCommerce ή e-comm, ορίζεται το εμπόριο παροχής αγαθών και υπηρεσιών που πραγματοποιείται εξ αποστάσεως με ηλεκτρονικά μέσα, βασιζόμενο δηλαδή στην ηλεκτρονική μετάδοση δεδομένων, χωρίς να καθίσταται αναγκαία η φυσική παρουσία των συμβαλλομένων μερών, πωλητή-αγοραστή. Περιλαμβάνει το σύνολο των διαδικτυακών διαδικασιών: ανάπτυξης, προώθησης, πώλησης, παράδοσης, εξυπηρέτησης και πληρωμής για προϊόντα και υπηρεσίες. Το εύρος των ανταλλαγών που διεξάγονται ηλεκτρονικά, έχει αυξηθεί ασυνήθιστα με την ευρεία χρήση του Διαδικτύου. Η χρήση του εμπορίου διεξάγεται κατ'αυτόν τον τρόπο, παρακινώντας και απορροφώντας καινοτομίες στην ηλεκτρονική μεταφορά χρηματικών πόρων, στη διαχείριση της εφοδιαστικής αλυσίδας (supply chain management), στο διαδικτυακό μάρκετινγκ(Internet marketing), στη διεκπεραίωση διαδικτυακών διαδικασιών (online transaction processing), στην ανταλλαγή ηλεκτρονικών δεδομένων (electronic data interchange, EDI), στην καταγραφή συστημάτων διοίκησης (inventory management) και στην αυτοματοποίηση συστημάτων συγκέντρωσης δεδομένων.

5.1.1 Είδη ηλεκτρονικού εμπορίου

Αρχικά το ηλεκτρονικό εμπόριο ανάλογα των συμβαλλομένων μερών διακρίνεται στους ακόλουθους τύπους:

- **B2B**. Προφέρεται μπι-του-μπι, ή μπράβο-του-μπράβο. Πρόκειται για ευφυές αρκτικόλεξο του αγγλικού όρου «business to business» και αφορά ηλεκτρονικό εμπόριο που διενεργείται μεταξύ επιχειρήσεων.Αυτό μπορεί να είναι ανοιχτό σε όλα τα ενδιαφερόμενα μέρη (ανταλλαγή εμπορευμάτων) ή περιορισμένο σε συγκεκριμένους προκαθορισμένους συμμετέχοντες (ιδιωτική ηλεκτρονική αγορά).
- **B2C**. Προφέρεται μπι-του-σί ή μπράβο-του-τσάρλι. Πρόκειται ομοίως σε χρήση αρκτικόλεξο του αγγλικού όρου «business to consumer» που αφορά ηλεκτρονικό εμπόριο που διενεργείται μεταξύ επιχειρήσεων (προμηθευτών, ή παροχής υπηρεσιών) και καταναλωτών αυτών.Αυτός ο τύπος ηλεκτρονικού εμπορίου

διεξάγεται από εταιρίες όπως η amazon.com. Η ηλεκτρονική αγορά αποτελεί μία μορφή ηλεκτρονικού εμπορίου στην οποία ο αγοραστής συνδέεται απευθείας με τον υπολογιστή του πωλητή συνήθως μέσω internet. Δεν εμπλέκεται καμία ενδιάμεση υπηρεσία. Οι συναλλαγές, αγορά ή πώληση, ολοκληρώνονται ηλεκτρονικά και διαδραστικά σε πραγματικό χρόνο, όπως γίνεται με την amazon.com για τα νέα βιβλία. Παρόλα αυτά σε κάποιες περιπτώσεις ένας μεσάζοντας μπορεί να είναι παρών σε μία συναλλαγή, όπως γίνεται με τις συναλλαγές στο eBay.com.

- **Mobile E-commerce**: Αυτό αφορά το επιχειρούμενο ηλεκτρονικό τηλεφωνικό εμπόριο.

5.2 Μέθοδοι υποκλοπής

Πιστωτικές κάρτες

Η εκτεταμένη χρήση πιστωτικών καρτών για ηλεκτρονικές συναλλαγές - και όχι μόνο - που γίνεται στις μέρες μας, απαιτεί ιδιαίτερη προσοχή από τους χρήστες τους, μιας και ελλοχεύουν αρκετοί κίνδυνοι που μπορεί να οδηγήσουν στην υποκλοπή σημαντικών χρηματικών ποσών. Οι εμπορικές συναλλαγές μέσω του διαδικτύου έχουν γνωρίσει δραματική αύξηση τα τελευταία χρόνια, κυρίως λόγω της αύξησης των χρηστών του internet. Όλο και περισσότερος κόσμος χρησιμοποιεί το διαδίκτυο, συνεπώς όλο και περισσότερος κόσμος πραγματοποιεί τις καθημερινές του εμπορικές συναλλαγές διαδικτυακά. Ο χρήστης του διαδικτύου έχει πλέον τη δυνατότητα να παραγγέλλει το φαγητό του διαδικτυακά ή ακόμα και να κάνει τα ψώνια του σε «διαδικτυακό» super market.

Διαδικτυακές υποκλοπές στοιχείων πιστωτικών καρτών

Ο πιο συνήθης τρόπος για να αποκτήσει κάποιος τα στοιχεία της πιστωτικής μας κάρτας είναι γιατί εμείς θα του τα δώσουμε, συνήθως χωρίς καν να συνειδητοποιούμε ότι το κάνουμε. Είναι εξαιρετικά σπάνιο να «σπάσει» κάποιος κάποιον κωδικό μας, προκειμένου να αποκτήσει πρόσβαση στα στοιχεία της κάρτας. Η διαδικασία αυτή είναι ιδιαίτερα δύσκολη, αφού απαιτεί ειδικές γνώσεις και ειδικά χρονοβόρα

λογισμικά και συνήθως δεν αξίζει τον κόπο, μόνο και μόνο για να αποκτήσει κάποιος τα στοιχεία μιας πιστωτικής κάρτας. Είναι αρκετά πιο εύκολο και αποδοτικό να ξεγελάσει κάποιος με διάφορους τρόπους τους χρήστες του διαδικτύου και να τους πείσει να δώσουν τα στοιχεία της πιστωτικής τους κάρτας ή και άλλα προσωπικά στοιχεία. Ας δούμε όμως τις πιο συνηθισμένες μεθόδους που χρησιμοποιούν οι επιτήδειοι, προκειμένου να ξεγελάσουν τους ανυποψίαστους χρήστες του διαδικτύου.

Τραπεζικοί οργανισμοί

Μία κλασική μέθοδος η οποία χρησιμοποιείται συχνότατα, είναι η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mails) σε χιλιάδες χρήστες, τα οποία υποτίθεται ότι προέρχονται από τον τραπεζικό τους οργανισμό. Αναφέρεται συνήθως στα μηνύματα αυτά ότι έχει προκύψει κάποιο πρόβλημα με το λογαριασμό τους ή με την πιστωτική τους κάρτα και ότι η τράπεζα χρειάζεται να επαληθεύσει τα στοιχεία ταυτότητας και τα στοιχεία πιστωτικής κάρτας. Θα πρέπει λοιπόν να αναφέρουμε στο σημείο αυτό, ότι οι συντάκτες αυτών των μηνυμάτων μελετούν τη φρασεολογία και το λεξιλόγιο που χρησιμοποιείται στις γνήσιες ιστοσελίδες των τραπεζών και φροντίζουν να είναι το ίδιο, ενώ οι λογαριασμοί ηλεκτρονικού ταχυδρομείου που δημιουργούν, μοιάζουν με αυτούς των τραπεζών. Τα μηνύματα αυτά, λοιπόν, είναι ιδιαίτερα πειστικά και αν ο χρήστης δεν είναι προσεκτικός, μπορεί εύκολα να ξεγελαστεί και να δώσει τα στοιχεία ταυτότητάς του και κυρίως τα πλήρη στοιχεία της πιστωτικής του κάρτας. Από αυτήν τη στιγμή και μετά, τα στοιχεία αυτά χρησιμοποιούνται για διαδικτυακές κυρίως αγορές, μέχρι ο χρήστης να το αντιληφθεί και να ακυρώσει την κάρτα. Υπήρξαν περιπτώσεις όπου χρήστες είχαν υψηλό πιστωτικό όριο στις κάρτες τους και έτσι «χρεώθηκαν» με αρκετές χιλιάδες ευρώ. Εκατομμύρια χρήστες του διαδικτύου ανά τον κόσμο, έχουν ξεγελαστεί με αυτόν τον τρόπο, έχουν δώσει τα στοιχεία της πιστωτικής τους κάρτας και εν συνεχεία, οι δράστες την έχουν «χρεώσει» πολλές φορές, μέχρι να φθάσει στο όριό της ή μέχρι να ακυρωθεί από τον πραγματικό κάτοχο.

On line αγγελίες-δημοπρασίες

Μία άλλη μέθοδος η οποία χρησιμοποιείται, είναι αυτή των on line αγγελιών και δημοπρασιών. Υπάρχουν πάρα πολλές ιστοσελίδες, στις οποίες ο καθένας μπορεί να αναρτήσει μία αγγελία ή να κάνει μία δημοπρασία για ένα προϊόν που θέλει να

πωλήσει. Σε αυτές τις συναλλαγές, πολλές είναι οι φορές όπου ζητείται από τον ανυποψίαστο αγοραστή να πληρώσει το αντίτιμο με την πιστωτική του κάρτα. Εδώ χρειάζεται ιδιαίτερη προσοχή, αφού αν δώσει τα στοιχεία της κάρτας του, μπορεί ο πωλητής να αποκτήσει πρόσβαση σε αυτά και από εκεί και πέρα να τη χρησιμοποιήσει ο ίδιος ή άλλο τρίτο πρόσωπο. Τα τελευταία χρόνια έχουν αναπτυχθεί ειδικές μέθοδοι τις οποίες εφαρμόζουν οι ιστοσελίδες δημοπρασιών, με τις οποίες ο πωλητής δεν έχει πρόσβαση στα προσωπικά στοιχεία (και στοιχεία της πιστωτικής κάρτας) του αγοραστή. Οι χρήστες λοιπόν, θα πρέπει να είναι ιδιαίτερα προσεκτικοί και σχολαστικοί σε αυτού του είδους τις αγορές και να φροντίζουν να ακολουθούν πιστά τις οδηγίες και τους τρόπους πληρωμής, τους οποίους προτείνουν οι ιστοσελίδες δημοπρασιών. Υποκλοπή προσωπικών στοιχείων και στοιχείων πιστωτικής κάρτας γίνεται και σε αγγελίες εργασίας. Χιλιάδες μηνύματα ηλεκτρονικού ταχυδρομείου στέλνονται σε χρήστες, τα οποία υποτίθεται ότι προέρχονται από μεγάλες εταιρείες, οι οποίες αναζητούν συνεργάτες σε όλον τον κόσμο. Και σε αυτά τα μηνύματα, η φρασεολογία και το λεξιλόγιο που χρησιμοποιούνται είναι ιδιαίτερα πειστικά. Όταν ο χρήστης λοιπόν ξεγελαστεί και απαντήσει σε ένα τέτοιο μήνυμα, του αποστέλλεται με καινούριο e-mail το συμβόλαιο-σύμβαση που πρέπει να υπογράψει με την υποτιθέμενη εταιρεία, προκειμένου να προσληφθεί. Μέσα στο συμβόλαιο αυτό, βέβαια, του ζητείται να αναγράψει τα πλήρη στοιχεία ταυτότητάς του, τραπεζικούς λογαριασμούς, αριθμούς πιστωτικών καρτών και άλλα και εν συνεχεία να το αποστείλει προκειμένου να εγκριθεί και να προσληφθεί πλέον στην εταιρεία. Τα συμβόλαια αυτά αποτελούν συνήθως αντιγραφές πραγματικών συμβολαίων με αλλαγμένα στοιχεία, συνεπώς είναι ιδιαίτερα πειστικά. Όταν ο χρήστης, λοιπόν, αποστείλει αυτά τα συμβόλαια με όλα του τα στοιχεία, οι δράστες τα χρησιμοποιούν αναλόγως για τη διάπραξη απατηλών συναλλαγών.

Ύποπτες ιστοσελίδες

Είναι αρκετές οι περιπτώσεις όπου έχουν παραβιαστεί οι βάσεις δεδομένων ιστοσελίδων και έχουν υποκλαπεί τα στοιχεία πιστωτικών καρτών των χρηστών και πελατών τους. Συνήθως είναι ιστοσελίδες, οι οποίες παρέχουν πρόσβαση και συνδρομές σε πορνογραφικό υλικό και ιστοσελίδες on line στοιχημάτων. Είναι

αρκετές οι περιπτώσεις ανά τον κόσμο, όπου εκλάπησαν τα στοιχεία πιστωτικών καρτών χρηστών, οι οποίοι εγγράφηκαν συνδρομητές σε ιστοσελίδες πορνογραφίας ή πλήρωσαν με την πιστωτική τους κάρτα για on line στοιχήματα. Σημειώνουμε στο σημείο αυτό, ότι δεν είναι όλες οι ιστοσελίδες πορνογραφικού υλικού και στοιχημάτων μη ασφαλείς και φυσικά έχουν παρατηρηθεί απώλειες στοιχείων πιστωτικών καρτών και σε άλλες ιστοσελίδες διαφορετικού περιεχομένου. Καλό θα ήταν ο χρήστης πριν εγγραφεί συνδρομητής σε μία οποιαδήποτε ιστοσελίδα και δώσει τα στοιχεία της πιστωτικής του κάρτας, να κάνει μία διαδικτυακή έρευνα για τη συγκεκριμένη ιστοσελίδα. Αν έχει υπάρξει «ρήγμα ασφαλείας» στη βάση δεδομένων της, είναι σχεδόν βέβαιο ότι θα αναφέρεται κάπου στο διαδίκτυο.

Trojan Horses

Η πιο δύσκολη - ίσως - από τεχνικής απόψεως μέθοδος υποκλοπής στοιχείων πιστωτικής κάρτας, είναι η τοποθέτηση ιών τύπου «Trojan Horse ή Data Loggers». Με τους ιούς αυτού του τύπου, μπορεί κάποιος να έχει πρόσβαση στον υπολογιστή του χρήστη και να υποκλέψει οτιδήποτε πληκτρολογεί. Συνεπώς, αν ο υπολογιστής κάποιου χρήστη έχει «μολυνθεί» από κάποιον τέτοιο ιό, δεν το αντιληφτεί και πληκτρολογήσει κωδικούς και στοιχεία της πιστωτικής του κάρτας, τρίτα άτομα που έχουν πρόσβαση στον υπολογιστή του εκείνη τη στιγμή, μπορούν να υποκλέψουν τα στοιχεία αυτά και να τα χρησιμοποιήσουν σε απατηλές συναλλαγές.

Υποκλοπή στοιχείων μπορεί να γίνει επίσης και αν πραγματοποιείται συναλλαγή σε μία ιστοσελίδα, χωρίς να υπάρχει ασφαλής σύνδεση. Αν ο χρήστης συμπληρώνει τις φόρμες των στοιχείων του, όπου αναγράφει και τα στοιχεία της πιστωτικής του κάρτας και η σύνδεσή του δεν είναι ασφαλής (το ότι ο χρήστης βρίσκεται σε ασφαλή σύνδεση με μία συγκεκριμένη ιστοσελίδα, φαίνεται είτε από το πλαίσιο στο οποίο αναγράφεται το όνομα-url της ιστοσελίδας, το οποίο συνήθως γίνεται κίτρινο και αναγράφεται αντί για http, https, ενώ εμφανίζεται και ένα μικρό λουκέτο στο κάτω δεξιό σημείο της ιστοσελίδας), τότε υπάρχει περίπτωση τρίτα άτομα να έχουν πρόσβαση εκείνη τη στιγμή στον υπολογιστή του και να υποκλέψουν τα στοιχεία της πιστωτικής του κάρτας.

Συμπερασματικά

Οι ανωτέρω μέθοδοι υποκλοπής στοιχείων πιστωτικών καρτών είναι ενδεικτικές και, φυσικά, όχι οι μόνες. Οι κάτοχοι πιστωτικών καρτών θα πρέπει να είναι ιδιαίτερα προσεκτικοί όταν τις χρησιμοποιούν, είτε εκτός είτε εντός διαδικτύου. Είδαμε παραπάνω πόσο εύκολο είναι για κάποια άτομα να υποκλέψουν τα στοιχεία της πιστωτικής μας κάρτας. Παραθέτουμε παρακάτω κάποιες προτάσεις, οι οποίες θα μας βοηθήσουν όσο είναι δυνατό να διαφυλάξουμε τα στοιχεία της πιστωτικής μας κάρτας.

- Θα πρέπει λοιπόν να βρισκόμαστε σε συνεχή επαφή με την τράπεζά μας, προκειμένου να ελέγχουμε την κίνησή της (ειδικά αν τη χρησιμοποιούμε συχνά).
- Να μη χάνουμε - όσο μπορούμε - την οπτική επαφή μαζί της, στις συναλλαγές μας σε καταστήματα.
- Να ζητούμε από τον τραπεζικό οργανισμό που συνεργαζόμαστε, να μας ενημερώνει τηλεφωνικά σε κάθε «περίεργη» ή μη συνηθισμένη κίνηση της κάρτας μας.
- Να ελέγχουμε την αξιοπιστία των ιστοσελίδων πριν τους «δώσουμε» τα στοιχεία της κάρτας μας και τα προσωπικά μας στοιχεία.
- Να εξετάζουμε συχνά τον υπολογιστή μας για ύπαρξη ιών και ειδικά πριν διενεργήσουμε μία διαδικτυακή συναλλαγή.
- Να είμαστε προσεκτικοί και σχολαστικοί σε ό,τι αφορά στις οικονομικές μας συναλλαγές μέσω του διαδικτύου, να μην εμπιστευόμαστε εύκολα κανέναν και να επαληθεύουμε τα πάντα.
- Να χρησιμοποιούμε προπληρωμένες κάρτες (prepaid cards)

Πλην των πιστωτικών καρτών, μπορούμε να χρησιμοποιούμε και τις λεγόμενες προπληρωμένες κάρτες. Οι κάρτες αυτές δεν είναι πιστωτικές. Λειτουργούν σαν κάρτες ταμιευτηρίου. Ο χρήστης αποταμιεύει σε αυτές χρήματα και εν συνεχεία μπορεί να κάνει αγορές, αξίας μέχρι και τα χρήματα που έχει αποταμιεύσει. Η λειτουργία τους είναι ανάλογη με αυτήν της καρτοκινητής τηλεφωνίας. Ουσιαστικά, ο χρήστης «φορτώνει» την κάρτα του και εν συνεχεία τη χρησιμοποιεί μέχρι να

«αδειάσει». Το πλεονέκτημα σε αυτές τις κάρτες έγκειται στο ότι αν κάποιος υποκλέψει τα στοιχεία τους, μπορεί να πάρει μόνο το ποσό που έχει αποταμιεύσει ο χρήστης. Οι κάρτες αυτές λοιπόν, ενδείκνυνται μόνο αν ο χρήστης αποταμιεύει μικρά ποσά σε αυτές (συνεπώς σε περίπτωση κλοπής των στοιχείων τους, θα έχει μικρή απώλεια χρημάτων). Προτείνεται για τους χρήστες αυτών των καρτών να αποταμιεύουν το ακριβές ποσό της αγοράς που επιθυμούν να πραγματοποιήσουν, λίγο πριν την πραγματοποιήσουν και μετά να αφήνουν την κάρτα χωρίς ή με ελάχιστα χρήματα.

Οι παραπάνω προτάσεις θα μας βοηθήσουν να εξασφαλίσουμε όσο είναι δυνατόν τις συναλλαγές μας με πιστωτικές κάρτες, θα πρέπει όμως όλοι μας να έχουμε υπόψη ότι μέχρι στιγμής είναι κοινά αποδεκτό ότι 100% ασφαλής συναλλαγή δεν υπάρχει. Υπάρχουν τρόποι και μέθοδοι να αυξήσουμε αρκετά την ασφάλεια των συναλλαγών μας, χωρίς όμως να φθάνουμε στο 100%. Γι' αυτό λοιπόν, ο καλύτερος τρόπος εξασφάλισής μας είναι το να απαιτούμε να ενημερωθούμε για κάθε τι καινούριο και να επαγρυπνούμε, προκειμένου να αποφύγουμε την ταλαιπωρία αλλά και το άγχος συναλλαγών, τις οποίες εμείς δεν πραγματοποιήσαμε ποτέ.

5.3 Ηλεκτρονικό Εμπόριο και Ασφάλεια

Ένα από τα πιο σημαντικά ζητήματα που σχετίζονται άμεσα με τη χρήση και τη διάδοση του Ηλεκτρονικού Εμπορίου αφορά το επίπεδο ασφάλειας των ηλεκτρονικών συναλλαγών.

Οι βασικές απαιτήσεις για την ασφαλή διεξαγωγή του Ηλεκτρονικού Εμπορίου είναι η Εμπιστευτικότητα (Confidentiality), η Ακεραιότητα (Integrity), και ο Έλεγχος Αυθεντικότητας (Authentication).

- **Εμπιστευτικότητα (Confidentiality).** Η εμπιστευτικότητα είναι απαραίτητο στοιχείο της ιδιωτικότητας του χρήστη (user privacy) καθώς και της προστασίας των μυστικών πληροφοριών. Η εμπιστευτικότητα είναι συνυφασμένη με την αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας και παρέχεται μέσω κρυπτογράφησης. Σε ένα ηλεκτρονικό

περιβάλλον θα πρέπει να υπάρχει η βεβαιότητα ότι το περιεχόμενο των μηνυμάτων που ανταλλάσσονται παραμένει αναλλοίωτο.

- **Ακεραιότητα (Integrity)**. Ακεραιότητα σημαίνει αποφυγή μη εξουσιοδοτημένης τροποποίησης των πληροφοριών που ανταλλάσσονται και παρέχεται μέσω ψηφιακής υπογραφής. Τα δεδομένα που αποστέλλονται ως μέρος της συναλλαγής πρέπει να είναι μη τροποποιήσιμα κατά τη διάρκεια της μεταφοράς και αποθήκευσής τους στο δίκτυο.
- **Έλεγχος Αυθεντικότητας (Authentication).** Η διαδικασία επαλήθευσης της ορθότητας του ισχυρισμού ενός χρήστη ότι κατέχει μια συγκεκριμένη ταυτότητα, αλλά και η βεβαιότητα ότι το περιεχόμενο του μηνύματος παρέμεινε αναλλοίωτο κατά την μεταφορά οριοθετούν την έννοια του ελέγχου αυθεντικότητας . Σύμφωνα με τον παραπάνω ορισμό η πιστοποίηση της ταυτότητας των επιχειρήσεων που συμμετέχουν σε μία συναλλαγή είναι απαραίτητη ώστε, κάθε συναλλασσόμενο μέρος να μπορεί να πεισθεί για την ταυτότητα του άλλου. Ο έλεγχος αυθεντικότητας παρέχεται μέσω ψηφιακής υπογραφής.
- **Εξουσιοδότηση (Authorization)**. Η εξουσιοδότηση αφορά την παραχώρηση δικαιωμάτων από τον ιδιοκτήτη στον χρήστη. Για παράδειγμα, ο πελάτης εξουσιοδοτεί τον έμπορο ώστε ο τελευταίος να ελέγξει αν ο αριθμός της πιστωτικής κάρτας είναι έγκυρος και αν τα χρήματα στον λογαριασμό μπορούν να καλύψουν το ποσό των συναλλαγών.
- **Εξασφάλιση (Assurance).** Η εμπιστοσύνη, ότι κάποιος αντικειμενικός σκοπός ή απαίτηση επιτυγχάνονται. Για παράδειγμα, μια από τις απαιτήσεις του πελάτη είναι η βεβαιότητα ότι ο έμπορος με τον οποίο συναλλάσσεται είναι νόμιμος και έμπιστος.
- **Μη αποποίηση ευθύνης (Non-repudiation).** Κανένα από τα συναλλασσόμενα μέρη δεν πρέπει να έχει τη δυνατότητα να αρνηθεί τη συμμετοχή του σε μια συναλλαγή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Εισαγωγή

“Ασφάλεια Δικτύων και Firewalls”, Ιστοσελίδα:

- http://www.logifer.gr/%CE%A4%CE%B5%CF%87%CE%BD%CE%B9%CE%BA%CE%AD%CF%82%CE%9B%CF%8D%CF%83%CE%B5%CE%B9%CF%82/%CE%A4%CE%B5%CF%87%CE%BD%CE%B9%CE%BA%CE%AE%CE%A5%CF%80%CE%BF%CF%83%CF%84%CE%AE%CF%81%CE%B9%CE%BE%CE%B7/%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CE%94%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD%CE%BA%CE%B1%CE%B9Firewalls/tabid/128/Default.aspx

Κεφάλαιο 1^{ο} : Ασφάλεια του Εξυπηρέτη Web

Βιβλίο: Βασικές Αρχές Ασφάλειας Δικτύων (2008), William Stallings

- Βιβλίο: Ασφάλεια Δικτύων Υπολογιστών (Κλειδάριθμος)

Κεφάλαιο 2^{ο} : Ασφάλεια του χρήστη

- Ιοί και σκουλήκια, Ιστοσελίδα:
  http://www.itsecurity.gr/security.html

- Antivirus, Ιστοσελίδα:
  http://www.free.gr/get/list.php?cat_id=16

- Avast, Εικόνα:
  https://www.google.gr/search?q=avast&es_sm=122&source=lnms&tbm=isch&sa=X&ved=0CAcQ_AUoAWoVChMI94fb2ciryAIVQQ4aCh0cGANW&biw=1366&bih=667#tbm=isch&q=avast+free+download&imgrc=_-Nyn3B84F8cXM%3A

- Avg Free, Εικόνα:
  https://www.google.gr/search?q=avast&es_sm=122&source=lnms&tbm=isch

&sa=X&ved=0CAcQ_AUoAWoVChMI94fb2ciryAIVQQ4aCh0cGANW&biw=1366&bih=667#tbm=isch&q=avg+free&imgdii=YG7N3FzPAgTyeM%3A%3BYG7N3FzPAgTyeM%3A%3BaXul-AZ8vLB3TM%3A&imgrc=YG7N3FzPAgTyeM%3A

- Panda, Εικόνα: https://www.google.gr/search?q=Panda+Cloud+Antivirus&es_sm=122&source=lnms&tbm=isch&sa=X&ved=0CAcQ_AUoAWoVChMIxa7qs8qryAIVy1YaCh358QDn&biw=1366&bih=667#imgrc=eeSWwttpt2eCKM%3A

- Microsoft Safety Scanner, Εικόνα: https://www.google.gr/search?q=Microsoft+Safety+Scanner&es_sm=122&source=lnms&tbm=isch&sa=X&ved=0CAcQ_AUoAWoVChMIxqHc98qryAIVSQ8aCh1yeggW&biw=1366&bih=667#imgrc=_PsMDfRC0X_UyM%3A

Κεφάλαιο 3^{ο} : Ψηφιακές Υπογραφές

- Ψηφιακές Υπογραφές, Ιστοσελίδα: http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html

- Δημόσιο Κλειδί, Ιστοσελίδα: https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%94%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

- Δημόσιο Κλειδί, Εικόνα: https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%94%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D#/media/File:%CE%93%CE%B5%CE%BD%CE%BD%CE%AE%CF%84%CF%81%CE%B9%CE%B1_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CF%8E%CE%BD.png

- Εμπιστευτικότητα Δημόσιου Κλειδιού, Εικόνα: https://upload.wikimedia.org/wikipedia/el/f/f4/%CE%9A%CF%81%CF%85%

CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%94%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D_-_%CE%95%CE%BC%CF%80%CE%B9%CF%83%CF%84%CE%B5%CF%85%CF%84%CE%B9%CE%BA%CF%8C%CF%84%CE%B7%CF%84%CE%B1.png

- Αυθεντικοποίηση Δημόσιου Κλειδιού, Εικόνα: https://upload.wikimedia.org/wikipedia/el/8/86/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%94%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D_-_%CE%91%CF%85%CE%B8%CE%B5%CE%BD%CF%84%CE%B9%CE%BA%CE%BF%CF%80%CE%BF%CE%AF%CE%B7%CF%83%CE%B7.png

- Συμμετρικό Κλειδί, Ιστοσελίδα: https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%A3%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%BF%CF%8D_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

- Κρυπτογράφηση Συμμετρικού Κλειδιού, Εικόνα: https://upload.wikimedia.org/wikipedia/el/a/a6/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%A3%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%BF%CF%8D_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D.png

- Πτυχιακή Εργασία (Αλγόριθμοι), Ιστοσελίδα: http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/kruptografia.htm

Κεφάλαιο 4ο : Φράγματα ασφαλείας (firewalls)

- Application Gateway, Εικόνα https://www.google.gr/search?q=application+gateway&espv=2&biw=1366&bih=667&source=lnms&tbm=isch&sa=X&ved=0CAYQ_AUoAWoVChMI-6252suyyAIVAnIaCh2EegFd#imgrc=qvXvtypL9E-aRM%3A

- Application Gateway, Ιστοσελίδα: http://users.ionio.gr/~emagos/THE%20WHOLE%20THING%202.pdf

- Εικονικά Ιδιωτικά Δίκτυα, Ιστοσελίδα: https://www.google.gr/search?q=virtual+private+network+configuration&espv=2&biw=1366&bih=667&source=lnms&tbm=isch&sa=X&ved=0CAYQ_AUoAWoVChMIxdiCzdCyyAIVBrwaCh1vxQKb#imgrc=Ti5Ed9j6NozlLM%3A

Κεφάλαιο 5ο : Ασφάλεια στο Ηλεκτρονικό Εμπόριο

- Ηλεκτρονικό Εμπόριο, Ιστοσελίδα: https://el.wikipedia.org/wiki/%CE%97%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C_%CE%B5%CE%BC%CF%80%CF%8C%CF%81%CE%B9%CE%BF

Πιστωτικές Κάρτες, Ιστοσελίδα:

- http://www.itsecuritypro.gr/contents_article.php?id=29&catid=4

- Ηλεκτρονικό Εμπόριο και Ασφάλεια, Ιστοσελίδα: www.icsd.aegean.gr/lecturers/gkorm/notes.doc