Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης
Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής και Πολυμέσων

Πτυχιακή Εργασία

Τίτλος

Μελέτη και δοκιμαστική λειτουργία των Μηχανισμών Ασφαλείας που παρέχει η πλατφόρμα Apple OSX Leopard.

ΗΛΙΑΣ ΜΑΝΤΟΥΒΑΛΟΣ (Α.Μ. 356)

ΗΡΑΚΛΕΙΟ – 15 ΔΕΚΕΜΒΡΙΟΥ 2009

Επόπτης Καθηγητής : Δρ. Μανιφάβας Χαράλαμπος

Υπεύθυνη Δήλωση: *Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους καθηγητές μου, που είχα το προνόμιο και την τιμή να παρευρίσκομαι στα μαθήματά τους και ιδιαίτερα τον κύριο Μανιφάβα για την ανεξάντλητη υπομονή του στην συγκεκριμένη πτυχιακή. Ένα μεγάλο ευχαριστώ και στους γονείς μου και ιδιαίτερα σε εκείνον που πλέον δεν είναι μαζί μας. Δίχως το κουράγιο τους δεν θα ήταν δυνατόν να ανασυντάξω τις δυνάμεις μου και να ολοκληρώσω το συγκεκριμένο πόνημα. Τέλος, ευχαριστώ και την Apple που παράγει και προωθεί προϊόντα που μας υπενθυμίζουν ότι η τεχνολογία υπάρχει για να μας υπηρετεί και όχι το αντίστροφο.

Ιστορικό εκδόσεων

Ημερομηνία	**Εκδοση**	**Συγγραφέας**	**Λεπτομέρειες**
09/10/2009	1.0	Ηλίας Μαντούβαλος	Αρχική έκδοση με ομαδοποίηση όλων των κεφαλαίων και αρχικό στήσιμο θεμάτων.
10/10/2009	1.1	Ηλίας Μαντούβαλος	Προσάρτηση των διαφανειών.
10/12/2009	1.2	Ηλίας Μαντούβαλος	Εφαρμογή των υποδείξεων.
14/12/2009	1.3	Ηλίας Μαντούβαλος	Τελική έκδοση.

Πίνακας περιεχομένων

Πίνακας εικόνων

Πίνακας πινάκων

Περίληψη

Ο κόσμος της πληροφορικής έχει διανύσει πολλά χρόνια πειραματισμών και προόδου όπου κύριο γνώρισμά τους είναι η εντυπωσιακή ταχύτητα που ανασυγκροτούνται οι εκάστοτε κυρίαρχες δυνάμεις. Μέσα σε όλο το συναρπαστικό χάος που επικρατεί στον κλάδο μας, ένα όνομα φέρει μια διαχρονική αξία ποιότητας και συμβόλου. Η εταιρία Apple ιδρύθηκε στην αρχή του πληροφορικού τσουνάμι με αξίες και προδιαγραφές διαφορετικές σε σχέση με τους ανταγωνιστές της. Οι επιλογές της είχαν πολλές φορές το τίμημά τους, αλλά και τα σημαντικά οφέλη τους. Προβλήματα που ταλαιπωρούν προϊόντα ανταγωνιστών, έχουν εξαφανιστεί από τα αντίστοιχα της Apple και τελικά παραδίδουν μία ολοκληρωτική σχέση διαδραστικότητας στον χρήστη τους. Ο τομέας της ασφάλειας που θα ασχοληθούμε στο παρόν έγγραφο είναι μόνο μία πτυχή από την εμπειρία που προσφέρει η Apple. Η έννοια του μπαλώματος και των ιών είναι ξένη στα λειτουργικά συστήματα της Apple, όπου δεν φοβάται να κάνει ριζικές αλλαγές στα συστήματά της προκειμένου να είναι καινοτόμος και διαμορφωτής του πληροφοριακού κόσμου.

Η παρούσα πτυχιακή είναι χωρισμένη σε τρία βασικά μέρη που στοχεύουν σε διαφορετικές πτυχές της ασφάλειας του λειτουργικού συστήματος

1. **Ασφάλεια του Υπολογιστή**. Τι ασφάλεια μας παρέχει το λειτουργικό σύστημα απέναντι σε δικές μας λάθος αποφάσεις ή σε περιπτώσεις που επιχειρείται πρόσβαση από φυσική παρουσία στον υπολογιστή μας

2. **Ασφάλεια Δικτύου**. Το επίπεδο ασφάλειας που μας παρέχεται σε δικτυακές και διαδικτυακές επιθέσεις από τρίτους.

3. **Ασφάλεια Εφαρμογών.** Γενική επισκόπηση και συμβουλές για την θωράκιση των βασικών προγραμμάτων του λειτουργικού συστήματος από εξωτερικές απειλές.

1. Εισαγωγή

Σκοπός Μελέτης

Όταν αναφερόμαστε στους υπολογιστές της Apple, στην ουσία αναφερόμαστε σε μία ιδεολογία στον τρόπο χειρισμού και παραγωγικότητας των καθημερινών μας ασχολιών. Είναι κοινά αποδεκτό ότι η συγκεκριμένη εταιρεία βρίσκεται πάντα στην πρώτη γραμμή των καινοτομιών, όχι μόνο από τεχνολογικής άποψης, αλλά και από τους τομείς αισθητικής και λειτουργικότητας. Καμία άλλη εταιρία στο χώρο των υπολογιστών έχει τοποθετήσει το desing σε τόσο υψηλή προτεραιότητα, όσο η Apple. Αυτό γίνεται άμεσα αντιληπτό από το λειτουργικό της σύστημα. Η εμμονή στην τελειότητα φαίνεται από το γεγονός ότι η ίδια η Apple δημιούργησε και εξέλιξε το δικό της λειτουργικό σύστημα για τα μηχανήματά της. Ένα λειτουργικό σύστημα που είναι παλαιότερο, σταθερότερο και κομψότερο από το αντίστοιχο των PC's, τα Windows σε όλες τους τις εκδόσεις.

Ένα πλήρες λειτουργικό σύστημα που είναι μπροστά από τον ανταγωνισμό σε πολλούς τομείς, με έναν από τους βασικότερους, εκείνο της ασφάλειας. Η αλήθεια είναι ότι ενώ τα Windows βάλλονται και ταλαιπωρούνται από μυριάδες σχεδιαστικά προβλήματα, το Mac OS[1] πάντα είχε την λύση και την εναλλακτική προσέγγιση σε βασικούς τομείς. Στην έκδοσή που μελετάμε (Mac OSX 10.5 - Leopard), είναι κάτι σαν ένα μικρό θαύμα, όπου οι καταρρεύσεις, οι ιοί και τα κακόβουλα προγράμματα είναι άγνωστες λέξεις γι'αυτό. Σκοπός μας λοιπόν είναι να μελετήσουμε την προσέγγιση που εφαρμόζει το Mac OSX προκειμένου να αντιμετωπίσει όλα τα προβλήματα ασφαλείας που εμφανίζονται στα σύγχρονα λειτουργικά συστήματα.

[1] http://en.wikipedia.org/wiki/Mac_OS

1.1.1. Λίγα λόγια για το Mac OSX

Από την ίδια του την σχεδίαση, το Mac OSX επιτυγχάνει δύο αντιφατικούς στόχους. Δημιουργεί ένα εύχρηστο περιβάλλον όπου είναι σταθερό και ανθεκτικό στους λάθος χειρισμούς του χρήστη. Αρχάριοι χρήστες μπορούν να καθίσουν μπροστά από την οθόνη του υπολογιστή τους, να εντοπίσουν τα εργαλεία που χρειάζονται και αμέσως να ξεκινήσουν να δουλεύουν. Παρομοίως, οι έμπειροι χρήστες μπορούν να έχουν πλήρη πρόσβαση σε ένα UNIX περιβάλλον, σε ανεπτυγμένες δικτυακές δυνατότητες και σε ένα πλούτο από εφαρμογές ανοικτού λογισμικού, όπως Apache web Server, Perl, Postfix, και πολλές άλλες ισχυρές υπηρεσίες.

1.1.2. Ιστορική Αναδρομή[2]

Το λειτουργικό σύστημα της Apple ξεκίνησε την πορεία του από την δημιουργία της ίδιας της εταιρίας. Το Mac OS (Operating System) ήταν πάντα πρωτοπόρο στην αγορά λογισμικού. Δεν ήταν όμως εξίσου διαδεδομένο, λόγο της εμμονής της Apple να το περιορίζει μόνο σε υπολογιστές κατασκευασμένους από την ίδια. Δεν είναι λοιπόν μία εταιρία που παρέχει δωρεάν λογισμικό (βλ. Linux), ούτε του επιτρέπει να λειτουργεί σε τρίτους κατασκευαστές (βλ. Windows).

Αν και τα παραπάνω μπορεί να φαίνονται ως μειονεκτήματα, στην πραγματικότητα ήταν οι λόγοι που κατάστησαν την εταιρία βιώσιμη και διακριτή από τον ανταγωνισμό. Σε κάθε έκδοσή του, το Mac OS είχε απόλυτη συμβατότητα και καλύτερη διαχείριση μνήμης και υλικού. Ήταν η ίδια απλότητα και τα ειδικευμένα δημιουργικά εργαλεία που έκαναν δημοφιλείς τους υπολογιστές Mac στους καλλιτεχνικούς επαγγελματίες.

Η έλευση του OS X ξεκίνησε με την έκδοση Server το 1999. Ήταν ένα προσωπικό στοίχημα του Steve Jobs να μεταφέρει την εμπειρία του και τους συνεργάτες του από την προηγούμενη εταιρία του, την NeXT[3]. Το βασικό απόκτημα από αυτή την ενέργεια ήταν η απόκτηση του NextSTEP, ενός λειτουργικού συστήματος βασισμένου στο OpenBSD και στην ιδέα της αντικειμενοστρέφειας[4]. Όπως κάθε πρωτοποριακό σύστημα, έτσι και αυτό ήταν μια παταγώδης αποτυχία το 1985, μετά από 14 χρόνια όμως παρουσιαζόταν πιο δυνατό από ποτέ.

Τον Μάρτιο του 2001 παρουσιάζεται η πρώτη πλήρης έκδοση για προσωπικούς υπολογιστές και από τότε το λειτουργικό σύστημα δεν έχει σταματήσει να αναβαθμίζεται και να ενημερώνεται. Η λίστα με τις εκδόσεις είναι η ακόλουθη:

[2] http://en.wikipedia.org/wiki/History_of_Mac_OS_X

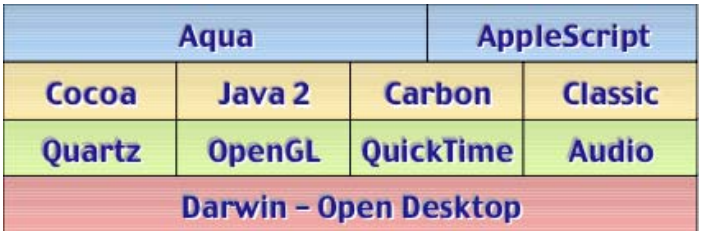
[3] http://www.nextcomputers.org/

[4] http://en.wikipedia.org/wiki/Object-oriented_programming

- Mac OS X Public Beta "Kodiak"
- Mac OS X v10.0 "Cheetah"
- Mac OS X v10.1 "Puma"
- Mac OS X v10.2 "Jaguar"
- Mac OS X v10.3 "Panther"
- Mac OS X v10.4 "Tiger"
- Mac OS X v10.5 "Leopard"
- Mac OS X v10.6 "Snow Leopard"

1.1.3. Δομή Συστήματος

Σαν γενική παραδοχή, μπορούμε να πούμε ότι το OSX είναι το νέο λειτουργικό σύστημα της Apple για την σειρά υπολογιστών Macintosh της ίδιας εταιρίας. Αν και διαδέχτηκε το λειτουργικό με το όνομα OS 9 , δεν αποτελεί απλά μια βελτιωμένη συνέχιση αυτού. Είναι χτισμένο εξολοκλήρου από το μηδέν και αποτελεί μια φρέσκια πρόταση στα λειτουργικά συστήματα. Ως χρήστης όμως, εκείνο που μας ενδιαφέρει, είναι η δυνατότητα να λειτουργήσουμε σωστά τις υπάρχουσες εφαρμογές, αλλά και καινούργιες ειδικά σχεδιασμένες για την συγκεκριμένη πλατφόρμα, όπως επίσης και εφαρμογές για Java και Unix. Με την έλευση των νέων Intel-Based Macintosh, τα πρώτα μοντέλα δηλαδή που ενσωματώνουν για πρώτη φορά επεξεργαστές αρχιτεκτονικής x86, υπάρχει η δυνατότητα να τρέξουμε και native εφαρμογές των Windows. Η παρακάτω εικόνα παραθέτει την δομή του OS X αρκετά καλά :



Εικόνα 1 - Δομή Συστήματος

Αν και το διάγραμμα είναι γεμάτο με άγνωστες λέξεις, στην πραγματικότητα είναι πολύ εύκολο να το κατανοήσουμε. Στην χαμηλότερη βαθμίδα (στην κόκκινη), είναι το Darwin[5], μία Unix βάση. Darwin είναι ο πυρήνας του λειτουργικού συστήματος, όπου είναι και της μορφής ανοιχτού λογισμικού[6]. Δηλαδή ο κώδικάς του είναι προσβάσιμος προς στο κοινό για έλεγχο και αποσφαλμάτωση. Είναι υπεύθυνος για βασικά τμήματα της λειτουργίας του συστήματος, όπως προστασία μνήμης και multitasking. Αν όμως το OS X ήταν μόνο Darwin, τότε θα είχαμε ένα σύστημα μόνο με γραμμή εντολών. Το πάνω κομμάτι (πράσινο), παρέχει τεχνολογίες υπεύθυνες για γραφικά και ήχο στο Darwin. Το χρυσό επίπεδο δείχνει τις διαφορετικές τεχνολογίες που οι developers μπορούν να χρησιμοποιήσουν προκειμένου να κατασκευάσουν εφαρμογές στο OS X. Τέλος, το μπλε επίπεδο είναι εκείνο που λαμβάνει ο τελικός χρήστης από το λειτουργικό σύστημα. Είναι η τελική διεπαφή όπου το σύστημα αλληλεπιδρά με τις εξωτερικές πηγές.

Ακόμα και αν δεν έχουμε χρησιμοποιήσει UNIX [7]στο OS X (κάτι πολύ πιθανό), τα πλεονεκτήματα που προσφέρει στις εφαρμογές των Mac, ειδικά στο τομέα της ασφάλειας, είναι πάμπολλα. Μπορείς να κάνεις πολλά πράγματα ταυτόχρονα (multitasking), χωρίς το φόβο κατάρρευσης (protected memory), και με καλύτερη

[5] http://www.puredarwin.org/

[6] http://www.opensource.apple.com/

[7] http://en.wikipedia.org/wiki/Unix

διαχείριση μνήμης (virtual memory) από τα αντίστοιχα ανταγωνιστικά λειτουργικά συστήματα. Το βασικότερο όμως, και εκείνο που θα ασχοληθούμε ενδελεχώς, είναι οι δικλίδες ασφαλείας που προσφέρει, τόσο ατομικά, όσο και σε επίπεδο δικτύου στην ραχοκοκαλιά του λειτουργικού συστήματος.

Με την ενσωμάτωση του Unix μέσα στη καρδιά του OS X, η Apple θωράκισε το λειτουργικό της σύστημα από διαδικτυακές επιθέσεις και ιούς. Ο λόγος είναι απλός και η σύγκριση αναπόφευκτη. Ενώ τα Windows ξεκίνησαν και αναπτύσσονταν με βασικό σκοπό να μείνουν μόνο σε έναν υπολογιστή και με ένα μόνο χρήστη, το Unix εξ' αρχής ήταν λειτουργικό που αποσκοπούσε στη δικτύωση και στους πολλούς χρήστες πάνω από έναν υπολογιστή. Η ιστορία δικαίωσε το πανεπιστημιακό λειτουργικό σύστημα, όπου εξ' αρχής είχε θέσει τις δικλίδες προστασίας στην διαδικτυακή λειτουργικότητα και στις προσβάσεις πάνω στο σύστημα από κακόβουλους εξωτερικούς παράγοντες. Εν' αντιθέσει, τα windows άργησαν να υλοποιήσουν την συγκεκριμένη προστασία περίπου 25 με 30 χρόνια, με την Microsoft είτε να αγνοεί, είτε να θέλει να "εξαγοράσει" το Internet για δικό της όφελος. Γι' αυτό, όλοι όσοι έχουν δουλέψει με τα Windows, έχουν την αίσθηση ενός λειτουργικού συστήματος με συνεχή "μπαλώματα[8]", όπου σέρνουν από πίσω τους τις λανθασμένες υλοποιήσεις και νοοτροπίες παλαιοτέρων εκδόσεων. Αν και έχουν βελτιωθεί τα λειτουργικά συστήματα της Microsoft, δεν πάει να υπάρχει ένα έλλειμμα τεχνογνωσίας στο θέμα διαδικτυακής ασφάλειας, κοντά στα 20 χρόνια.

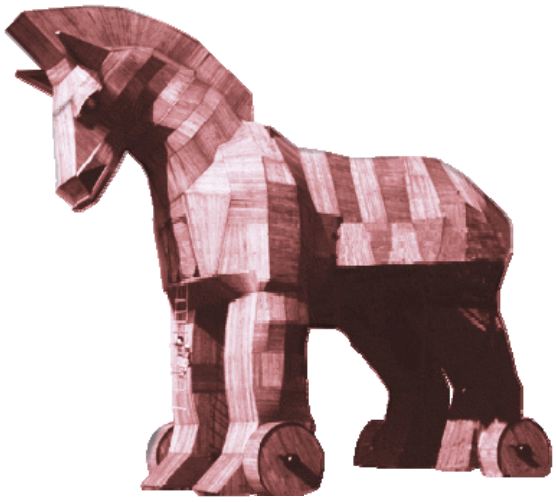
[8] http://www.microsoft.com/Security/

1.1.4. Σύστημα μελέτης

Η παρούσα μελέτη έγινε σε υπολογιστή MacMini με την έκδοση OS X Leopard 10.5.5 και τα κάτωθι χαρακτηριστικά :

Εικόνα 2 - Το σύστημά μας

1.2. UNIX Security



1.2.1. Γενικά

Κατά βάση, το MAC OSX είναι ένα πλήρες λειτουργικό σύστημα UNIX. Ο βασικός σχεδιασμός του UNIX ήταν εκείνος της προγραμματιστικής πλατφόρμας, δίχως ιδιαίτερη έμφαση στην ασφάλεια των αρχείων. Με τον καιρό, έγιναν προσπάθειες προκειμένου να καλυφθούν οι επιτακτικές ανάγκες στα κενά ασφαλείας που παρουσιαζόντουσαν και έτσι καταλήξαμε στο μοντέλο της ενσωμάτωσης flags στα ίδια τα αρχεία, προκειμένου να περιοριστούν οι ανεπιθύμητες προσβάσεις από τρίτους. Κάθε αρχείο ανήκει σε συγκεκριμένο χρήστη, κάθε πρόγραμμα εκτελείται από έναν συγκεκριμένο χρήστη.

1.2.2. Χρήστες και Ομάδες

Όπως και οι υπόλοιπες διανομές του UNIX, έτσι και το MAC OS X ενσωματώνει ένα σχετικά απλό μοντέλο χρήστη/ομάδας, όπου κάθε χρήστης και ομάδα αναπαριστώνται από έναν ακέραιο αριθμό, γνωστά και ως user identifier (UID) και group identifier (GID). Τα UID και GID είναι εκείνα που χρησιμοποιεί το λειτουργικό σύστημα για αναγνωριστικούς σκοπούς και κατά συνέπεια για να ασκήσει έλεγχο προσβασιμότητας στα αρχεία. Τα UID και GID τιμές αποθηκεύονται ως 32-bit ακέραιοι στο MAC OSX με την μέγιστη UID τιμή να είναι 2,147,483,647. Οι χρήστες και οι ομάδες έχουν δικά τους ονόματα, αλλά αυτό εξυπηρετεί περισσότερο ως διευκόλυνση προς τον χρήστη.

Οι UID τιμές δεν είναι απαραίτητο να είναι μοναδικές, αλλά τις περισσότερες φορές αυτό ισχύει. Αν βρεθούν λογαριασμοί χρηστών που έχουν το ίδιο UID, τότε δεν υπάρχει διαχωρισμός στα μεταξύ τους αρχεία. Με την ίδια λογική, μπορούμε να υποθέσουμε το ίδιο και για τις τιμές του GID, όπου δεν θα υπάρχει

διαχωρισμός των αρχείων μεταξύ εκείνων των ομάδων. Στις περιπτώσεις που υπάρξει περιστατικό κοινών τιμών, καλό θα ήταν από τον εκάστοτε administrator συστήματος να ερευνηθεί το γεγονός αυτό.

1.2.3. Πανομοιότυπα UIDs

Τις περισσότερες φορές που υφίσταται η χρήση πανομοιότυπων UID, είναι για να δημιουργήσουμε έναν εφεδρικό root λογαριασμό στην περίπτωση καταστροφής του συστήματος ή για να έχουμε πολλαπλά root accounts για πολλούς administrators. Παρόλα αυτά, μια τέτοια τεχνική διαχείρισης ενός υπολογιστικού συστήματος θα πρέπει να αποφεύγεται. Οι απλοί χρήστες θα πρέπει να έχουν πάντα μοναδικές UID τιμές. Η προτεινόμενη μέθοδος για να αποδώσουμε πρόσβαση αρχείων σε ένα πλήθος από χρήστες είναι εκείνη των κοινών ομάδων.

Οι χρήστες είναι μέλη ενός ή περισσοτέρων ομάδων. Κάθε χρήστης έχει μία βασική ομάδα όπου ανήκει. Μπορούμε να δούμε την ομάδα όπου ανήκει ο κάθε χρήστης με την εντολή groups.

```
bash-2.05a$ groups
staff admin
bash-2.05a$
```

Ο παραπάνω χρήστης είναι μέλος των ομάδων staff και admin. Η βασική ομάδα είναι η staff, αλλά κάτι τέτοιο δεν είναι άμεσα αντιληπτό από το παράδειγμα. Για καλύτερα αποτελέσματα, μπορούμε να χρησιμοποιήσουμε την εντολή id:

```
bash-2.05a$ id
uid=501(brian)   gid=20(staff)   groups=20(staff),
80(admin)
```

Αυτή η εντολή μπορεί να εμπλουτιστεί με περισσότερες πληροφορίες και μπορεί να γίνει πολύ χρήσιμη. Τα ονόματα όπως και οι τιμές των ID μπορούν να εμφανιστούν. Επιπροσθέτως, η βασική ομάδα του χρήστη αποκαλύπτεται. Αυτή η εντολή προαιρετικά λαμβάνει ένα όνομα χρήστη σαν όρισμα, οπότε μπορούμε να δούμε τις πληροφορίες για έναν συγκεκριμένο χρήστη. Για παράδειγμα :

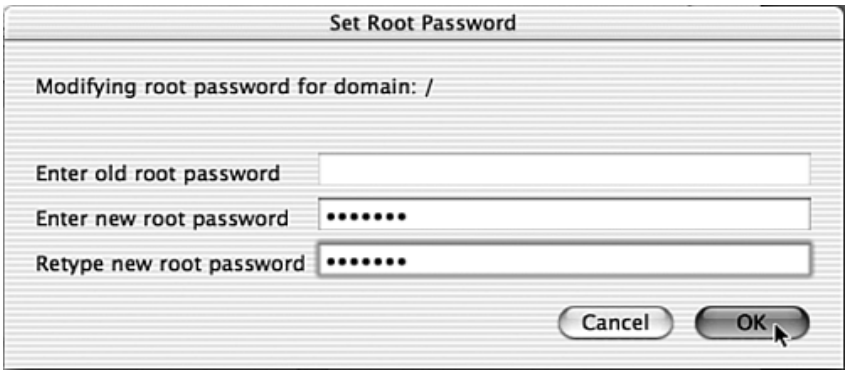
```
bash-2.05a$ id root
uid=0(root)      gid=0(wheel)      groups=0(wheel)
1(daemon) 2(kmem) 3(sys)
4(tty) 5(operator) 20(staff) 31(guest) 80(admin)
```

1.2.4. Τύποι χρηστών

Στον κόσμο του UNIX, τυπικά υπάρχουν δύο είδη χρηστών : οι κανονικοί χρήστες και οι υπερχρήστες ή root. Σαν προεπιλογή το Mac OSX δημιουργεί έναν υπερχρήστη και έναν administrator που έχει τα προνόμια του root χρήστη.

1.2.5. Root, ο υπερχρήστης

Δίχως καμία αμφιβολία, ο βασικότερος λογαριασμός χρήστη είναι εκείνος του root (UID 0), διότι ο χρήστης root μπορεί να κάνει σχεδόν τα πάντα. Είναι ο λογαριασμός που χρησιμοποιείται για να διαχειριστεί την εκκίνηση του συστήματος, άλλους λογαριασμούς, να διαχειριστεί τα αρχεία αλλά και το δίκτυο του συστήματος, αλλά και άλλα σημαντικά επίπεδα λειτουργίας. Αυτός ο λογαριασμός αναφέρεται και ως λογαριασμός συστήματος στον Finder. Λόγω των αυξημένων δυνατοτήτων για καταστροφικούς χειρισμούς, αυτός ο λογαριασμός δεν πρέπει να διαχειρίζεται ως κανονικός λογαριασμός, ούτε καν από τους administrators.



Εικόνα 3 – Παράθυρο Αλλαγής Κωδικού Root User

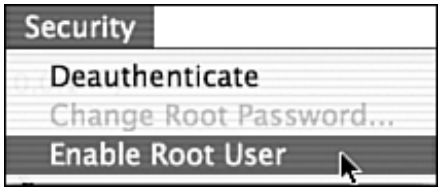
1.2.6. Οι ρόλοι του κάθε χρήστη

Για να μειώσουμε το ρίσκο της απειλής, θα πρέπει να εφαρμόζουμε τον κανόνα των ελάχιστων δικαιωμάτων. Σαν ιδανικό αποτέλεσμα θα έχουμε μόνο έναν λογαριασμό με δικαιώματα administrator. Δικαιώματα administrator μπορούμε να λάβουμε προσωρινά με την εντολή sudo. Η Apple εφαρμόζει τον παραπάνω κανόνα απενεργοποιώντας των root λογαριασμό ως προεπιλογή του συστήματος. Με αυτή την συνθήκη, δεν μπορούμε να έχουμε πρόσβαση στον root από την οθόνη login. Ο χρήστης που δημιουργείται κατά την εγκατάσταση λαμβάνει δικαιώματα administrator. Αυτός ο χρήστης ανήκει στην admin ομάδα και ως συνέπεια έχει λάβει τις δυνατότητες της εντολής sudo.

Ως προεπιλογή, ο λογαριασμός root είναι απενεργοποιημένος και δεν έχει κωδικό. Αμέσως μετά την εγκατάσταση, ο root πρέπει να ενεργοποιείται. Αυτό περιλαμβάνει την διαδικασία της ενεργοποίησης, την επιλογή κωδικού ασφαλείας και στην συνέχεια την απενεργοποίηση του λογαριασμού ξανά. Αυτό μπορεί να

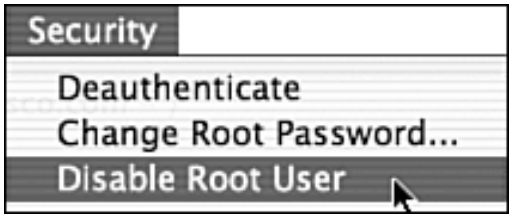
γίνει με την εφαρμογή NetInfo[9] Manager (/Applications/Utilities/NetInfo Manager.app).

1.2.7. Πιστοποίηση και ενεργοποίηση του root λογαριασμού



Εικόνα 4 - Παράθυρο Ενεργοποίησης root λογαριασμού

1.2.8. Πιστοποίηση και απενεργοποίηση του root λογαριασμού



Εικόνα 5 – Παράθυρο Απενεργοποίησης root λογαριασμού

Μετά την εκκίνηση του NetInfo Manager, θα πρέπει να ορίσουμε ένα admin username και password. Τώρα ο λογαριασμός root είναι απενεργοποιημένος και κανένας δεν μπορεί να μπει στο σύστημά μας ως root. Επίσης, ο κωδικός του root έχει τοποθετηθεί και (ελπίζουμε) να το ξέρει μόνο ο διαχειριστής.

Με το Mac OS X Server, ο λογαριασμός root είναι ενεργοποιημένος ως προεπιλογή, οπότε οι παραπάνω ενέργειες δεν εφαρμόζονται στην περίπτωσή του. Ο στόχος μας είναι να παρθούν όλες οι απαραίτητες ενέργειες ώστε να αποτρέψουμε εισαγωγή στον root λογαριασμό και κάτι τέτοιο μπορεί να γίνει αν τον απενεργοποιήσουμε.

[9] http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh1550.html

1.2.9. Διαχειριστές

Ο χρήστης που δημιουργήθηκε κατά την εγκατάσταση θεωρείται διαχειριστής. Αυτό σημαίνει ότι έχει τις δυνατότητες της εντολής sudo και ότι ανήκει στην ομάδα admin. Ο μόνος άλλος χρήστης σε αυτή την ομάδα είναι ο root, εκτός αν έχουμε προσθέσει χειροκίνητα και άλλους. Τα μέλη αυτής της ομάδας μπορούν να έχουν πρόσβαση στα αρχεία συστήματος και να εγκαθιστούν προγράμματα στον φάκελο Applications. Όλοι οι υπόλοιποι χρήστες έχουν δικαιώματα ανάγνωσης και εκτέλεσης στον φάκελο των εφαρμογών. Αυτό σημαίνει ότι δεν μπορούν να σώσουν, να μετατρέψουν ή να διαγράψουν κανένα από τα αρχεία.

Στο Mac OS X Server, ο χρήστης που δημιουργήθηκε κατά την εγκατάσταση είναι και ο διαχειριστής του συστήματος. Παρόλα αυτά, ο κωδικός που δόθηκε σε αυτόν τον χρήστη είναι επίσης και ο κωδικός του λογαριασμού root. Αυτό σημαίνει ότι ο λογαριασμός root έχει κωδικό και είναι ενεργοποιημένος. Παρόμοια, προτείνεται ο κωδικός root να αλλάξει ώστε να μην είναι ο ίδιος με τον κωδικό του διαχειριστή συστήματος, και στην συνέχεια να απενεργοποιηθεί.

Ως προεπιλογή, όλα τα μέλη της ομάδας admin έχουν πρόσβαση στο σύστημα όμοια με την εντολή sudo. Προκειμένου να περιορίσουμε τις περιττές και επικίνδυνες προσβάσεις στα αρχεία του συστήματός μας, καλό θα ήταν να έχουμε μόνο έναν λογαριασμό με δυνατότητα sudo. Δυστυχώς, στο Mac OS X, όλα τα μέλη της ομάδας admin έχουν την δυνατότητα sudo ως προεπιλογή και η αλλαγή αυτή της κατάστασης απαιτεί αλλαγές στα αρχεία συστήματος.

1.2.10. Ειδικοί χρήστες

Όταν έχουμε μια νέα δημιουργία χρήστη, τότε αυτός έχει τις προεπιλεγμένες τιμές UID 501. Στα περισσότερα UNIX συστήματα, χαμηλότερες τιμές είναι κατειλημμένες για χρήση του συστήματος. Στο Mac OS X αυτές είναι οι τιμές κάτω από 100. Οι συγκεκριμένοι λογαριασμοί χρηστών χρησιμοποιούνται για διάφορους σκοπούς και διαφέρουν σε κάθε διανομή UNIX. Η ιδέα είναι ότι βασικές εφαρμογές συστήματος χρειάζονται να λαμβάνουν άδειες πρόσβασης για να ολοκληρώσουν την λειτουργία τους και για να γίνει κάτι τέτοιο, πρέπει να δημιουργηθεί ένας χρήστης όπου πληρεί αυτές τις άδειες πρόσβασης και συνήθως είναι και ο ιδιοκτήτης των αρχείων που σχετίζονται με την συγκεκριμένη λειτουργία.

Ο παρακάτω πίνακας περιλαμβάνει τους λογαριασμούς συστήματος που εγκαθίστανται μαζί με το Mac OS X. Ορισμένοι από τους λογαριασμούς δεν δημιουργούνται, π.χ. ο λογαριασμός mmuser δημιουργείται μόνο αν ο Macintosh Management Server εκκινηθεί.

1.2.11. Πίνακας ειδικών χρηστών

UID	SHORT NAME	Περιγραφή
–17	mmuser	Διαχειριστής του Macintosh Management Server (Mac OS X Server μόνο).
–2	nobody	Ένας λογαριασμός δίχως δικαιώματα σε αρχεία η προσωπικό φάκελο.
0	root	Ο χρήστης με τα περισσότερα δικαιώματα, ο υπερχρήστης.
1	daemon	Διαχειριστής ειδικών εφαρμογών συστήματος με περιορισμένα δικαιώματα.
25	smmsp	Ο χρήστης που διαχειρίζεται την εφαρμογή sendmail.
70	www	Ο χρήστης που διαχειρίζεται τον εξυπηρετητή Apache.
74	mysql	Ο χρήστης που διαχειρίζεται τον εξυπηρετητή βάσεων δεδομένων MySQL.
75	sshd	Ο χρήστης που διαχειρίζεται τον εξυπηρετητή secure shell.
98	ftp	Ο χρήστης που χρησιμοποιούν οι συνδεδεμένοι ανώνυμοι χρήστες ftp.
99	unknown	Χρησιμοποιείται για άγνωστα volumes.

Πίνακας 1 - Πίνακας ειδικών χρηστών

1.2.12. Ειδικές Ομάδες

Όπως υπάρχουν ειδικοί λογαριασμοί χρηστών για χρήση από το ίδιο το σύστημα, έτσι υπάρχουν και ειδικές ομάδες για παρόμοια χρήση. Με αυτό τον τρόπο μπορούν να έχουν και μεμονωμένοι χρήστες πρόσβαση σε λειτουργίες που αφορούν υπηρεσίες του λειτουργικού μας συστήματος.

Ο παρακάτω πίνακας περιλαμβάνει τις ομάδες συστήματος που έρχονται εγκατεστημένες μαζί με το MAC OS X. Ορισμένες από αυτές είναι κληρονομούμενες από το UNIX και δεν χρησιμοποιούνται τόσο συχνά.

1.2.13. Ειδικές Ομάδες Συστήματος

GID	Όνομα	Περιγραφή
–2	`nobody`	Χρήση για ορισμένες υπηρεσίες συστήματος.
–1	`nogroup`	Χρήση για ορισμένες υπηρεσίες συστήματος.
0	`wheel`	Η βασική ομάδα του root.
1	`daemon`	Χρήση για ορισμένες υπηρεσίες συστήματος με περιορισμένα δικαιώματα.
2	`kmem`	Χρήση για την μνήμη του πυρήνα, π.χ. /dev/mem και /dev/kmem
3	`sys`	Δεν χρησιμοποιείται.
4	`tty`	Χρήση για διαχείριση αρχείων που σχετίζονται με απομακρυσμένες προσβάσεις και συγκεκριμένες εφαρμογές.
5	`operator`	Δεν χρησιμοποιείται.
6	`mail`	Χρήση για διαχείριση αρχείων mail.
7	`bin`	Χρήση για ιδιοκτησία δυαδικών αρχείων (κληροδοτούμενο από το UNIX).
20	`staff`	Η βασική ομάδα για όλους τους χρήστες.

25	smmsp	Η ομάδα που λειτουργεί την υπηρεσία sendmail.
31	guest	Η ομάδα του χρήστη όπου δεν έχει κανένα αρχείο.
45	utmp	Δεν χρησιμοποιείται.
66	uucp	Χρήση για διαχείριση uucp μεταφορών.
68	dialer	Χρήση για την διαχείριση modems.
69	network	Δεν χρησιμοποιείται.
70	www	Η ομάδα που διαχειρίζεται των εξυπηρετητή Apache.
74	mysql	Η ομάδα που διαχειρίζεται των εξυπηρετητή βάσεων δεδομένων MySQL.
75	sshd	The user that runs the secure shell server processes. Η ομάδα που διαχειρίζεται των εξυπηρετητή secure shell.
80	admin	Η ομάδα που περιλαμβάνει τους διαχειριστές του συστήματος. Ως προεπιλογή η συγκεκριμένη ομάδα έχει δυνατότητες sudo.
99	unknown	Χρήση για προσαρτημένα συστήματα αρχείων.

Πίνακας 2 – Πίνακας Ειδικών Ομάδων Συστήματος

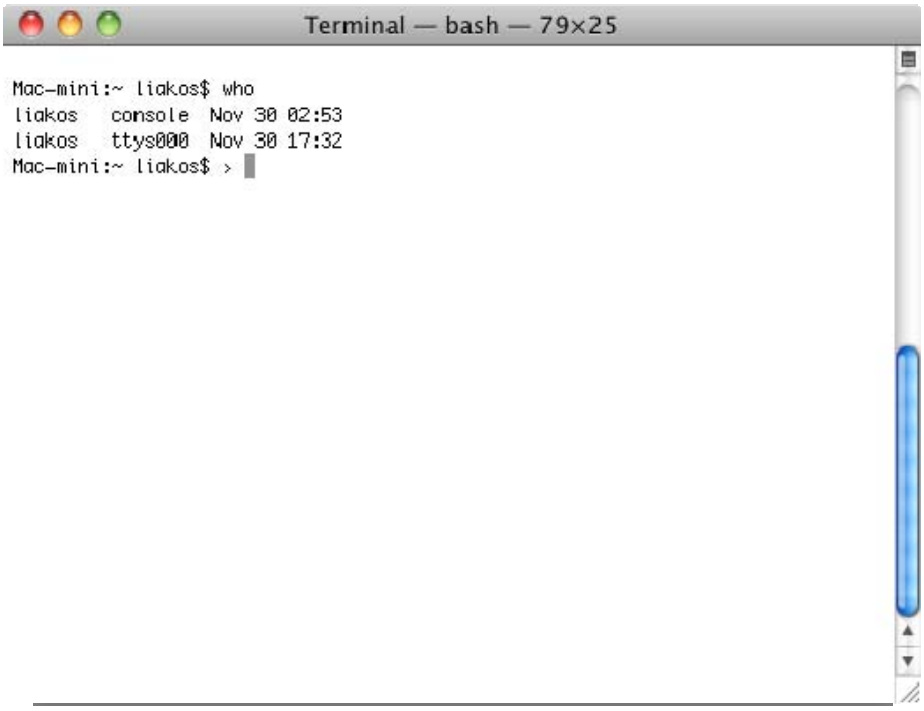
1.2.14. Εντολές για την διαχείριση χρηστών και ομάδων

Το Unix , και κατά συνέπεια το ίδιο το Mac OS X, μας προσφέρει μια πληθώρα εντολών που μας επιτρέπουν να διαχειριστούμε τους λογαριασμούς και τις ομάδες χρηστών. Μέσα από την εφαρμογή terminal[10] έχουμε πρόσβαση σε όλες τις ακόλουθες εντολές.

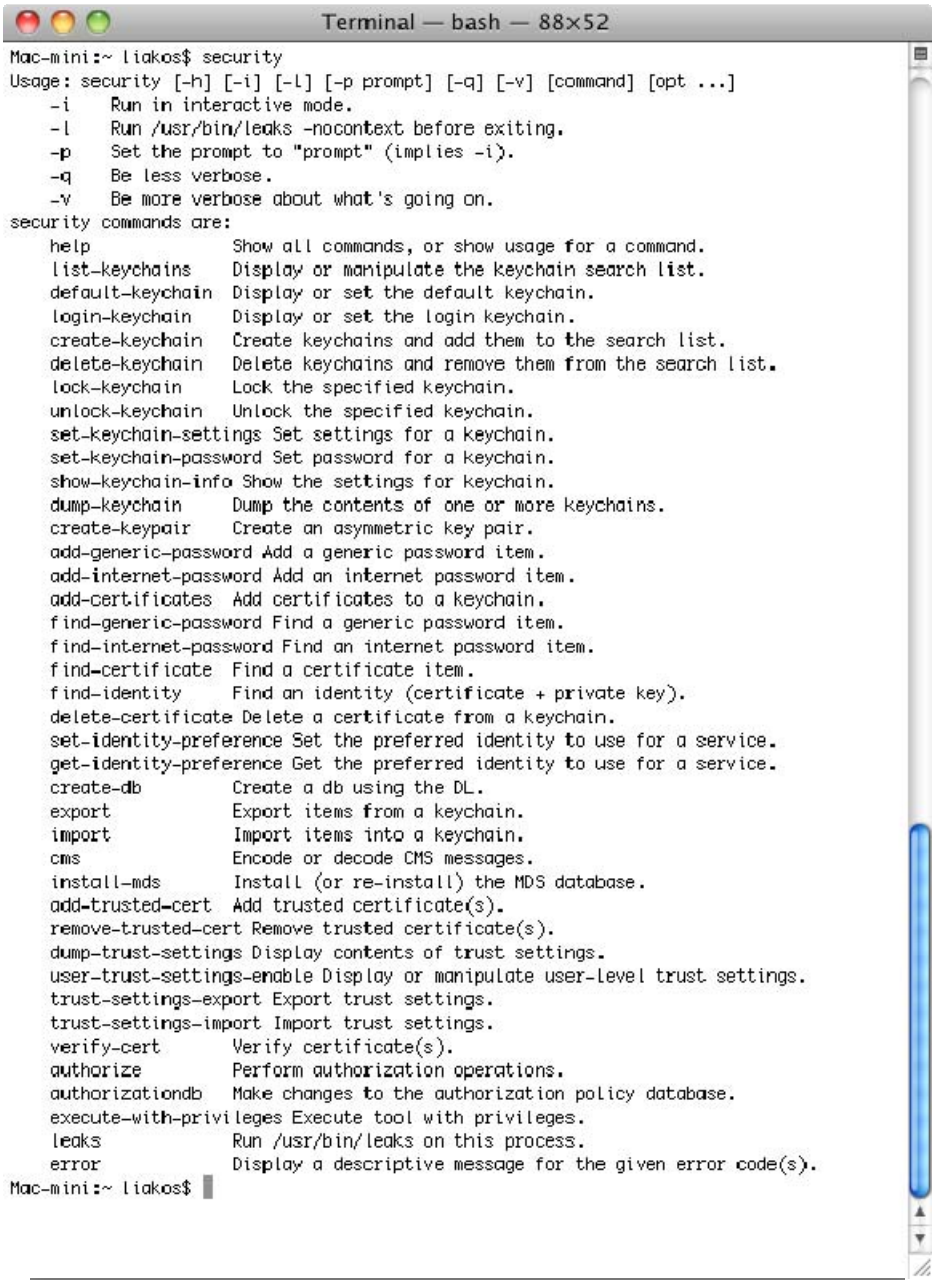
Εντολή	Περιγραφή
chgrp	Change group ownership
chmod	Change access permission
chown	Change file owner and group
groups	Print group names a user is in
id	Print user and group names/id's
Last	Indicate last logins of users and ttys
passwd	Modify a user password
security	Administer Keychains, keys, certificates and the Security framework
setfile	Set attributes of HFS+ files
su	Substitute user identity
sudo	Execute a command as another user
umask	Users file creation mask
which	Locate a program file in the user's path
who	Print all usernames currently logged on
whoami	Print the current user id and name (`id -un')
write	Send a message to another user

Πίνακας 3 - Εντολές διαχείρισης χρηστών

[10] /Applications/Utilities/Terminal.app



Εικόνα 6 - Αποτέλεσμα εντολής who



Εικόνα 7 - Παράμετροι εντολής security

2. Ασφάλεια Υπολογιστή

Η παρούσα ενότητα περιλαμβάνει διάφορες μεθόδους για περαιτέρω θωράκιση του Mac OS X από την σκοπιά του τοπικού χρήστη :

- Με την φυσική του παρουσία στο μηχάνημα.
- Με αλληλεπιδραστική τοπική χρήση μέσω υπηρεσιών όπως το Secure Shell (SSH) ή το Apple Remote Desktop (ARD).

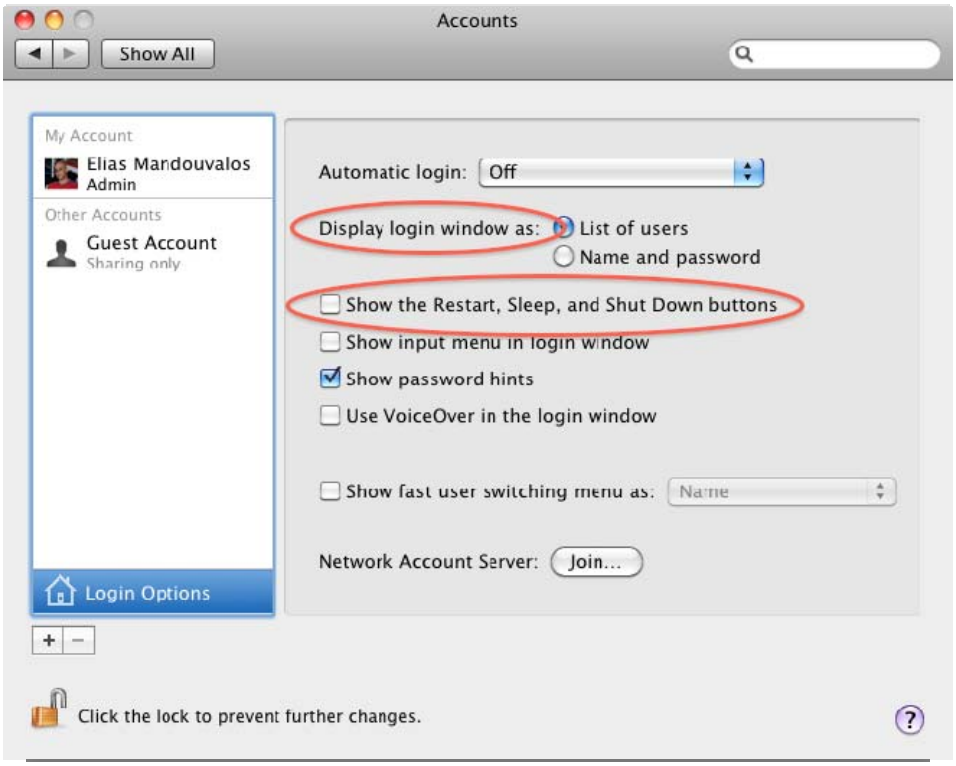
Εικόνα 8 – Παράθυρο Εισόδου

2.1. Το παράθυρο εισόδου-Login

Παρακάτω, θα εξετάσουμε μεθόδους για να ενεργοποιήσουμε και να κλειδώσουμε το παράθυρο εισόδου. Ως προεπιλογή, το Mac OS X αυτόματα εισάγει στο σύστημά του τον προεγκατεστημένο χρήστη αντί να τον αναγκάζει να πληκτρολογήσει κωδικό προκειμένου να πιστοποιήσει την αυθεντικότητά του.

2.1.1. Ενεργοποίηση και κλείδωμα του παραθύρου εισόδου.

Για να ενεργοποιήσουμε το παράθυρο εισόδου, να απενεργοποιήσουμε τα βοηθήματα κωδικών , να αποκτήσουμε πρόσβαση στις επιλογές τερματισμού/επανεκκίνησης και αυτόματης πρόσβασης, μπορούμε να επεξεργαστούμε το αρχείο /Library/Preferences/com.apple.loginwindow.plist ως διαχειριστές ή απλά να χρησιμοποιήσουμε το παράθυρο Accounts στον Πίνακα Ρυθμίσεων :



Εικόνα 9 - Παράθυρο Επιλογών Χρηστών

Εικόνα 10 - Users configuration file

- Apple menu -> System Preferences -> Accounts -> Login options ->
- "Display Login Windows as" -> "Name and Password"
- Uncheck "Automatically log in as:"
- Uncheck "Show the Sleep, Restart and Shut Down buttons"
- Uncheck "Enable fast users switching" if not used

Η επιλογή "Fast user switching" είναι χρήσιμη σε υπολογιστές με πολλούς χρήστες, αλλά σε περιβάλλοντα με έναν χρήστη δεν χρησιμοποιείται ποτέ και αποτελεί ένα πιθανό κενό ασφαλείας (π.χ. Μία απομακρυσμένη σύνδεση ως root μπορεί να χρησιμοποιήσει το Fast user switching για να βλάψει το σύστημα link).

Για να απενεργοποιήσουμε την αυτόματη είσοδο :

- Apple menu -> System Preferences -> Security
- Check "Disable automatic login"

Εικόνα 11 – Παράθυρο Ρυθμίσεων Ασφάλειας

Για να ενεργοποιήσουμε ένα μήνυμα κειμένου να εμφανίζεται ως μέρος το παραθύρου εισόδου, θα χρειαστεί να επεξεργαστούμε το αρχείο /Library/Preferences/com.apple.loginwindow.plist. Το αρχείο έχει την μορφή :

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>DisableConsoleAccess</key>
<true/>
<key>LoginwindowText</key>
<string>Authorized users only.</string>
```

Παρατηρήστε την γραμμή <string> κάτω από την καταχώρηση LoginwindowText. Εισάγετε το κείμενο που θέλετε να εμφανίζεται στο παράθυρο εισόδου και τερματίστε την καταχώρηση με την εντολή </string>.

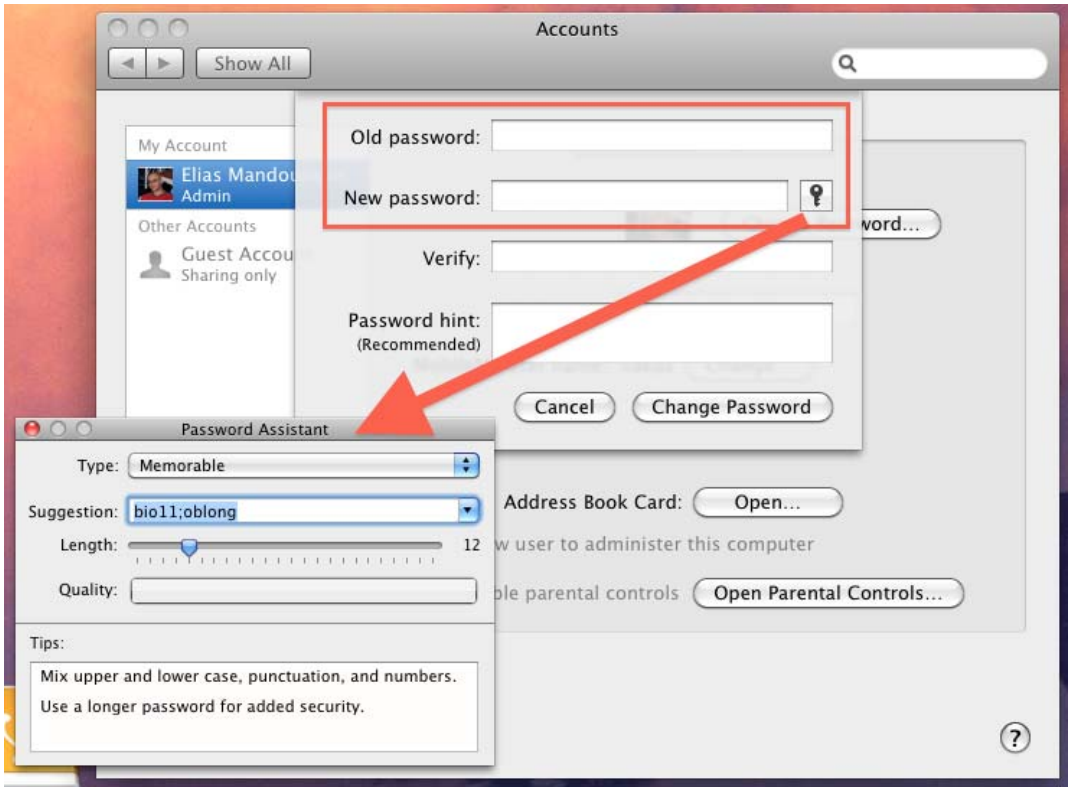
2.1.2. Αλλαγές κωδικών

Μια πολύ καλή πρακτική περαιτέρω εξασφάλισης, είναι η συχνή αλλαγή κωδικών χρήστη, ιδιαίτερα αν δεν υπάρχει κάποια κωδικοποίηση στον τρόπο που εισάγονται. Αυτό σημαίνει ότι κάποιος χρήστης με δικαιώματα διαχειριστή μπορεί να ανακτήσει τον κωδικό σας από τα αρχεία swap[11].

Γενικά, τα αρχεία swap συναντώνται σε πολλές πτυχές κατά την εργασία μας πάνω από τον υπολογιστή. Είναι αρχεία στο σκληρό δίσκο που σκοπό έχουν να κρατήσουν προσωρινές πληροφορίες για την λειτουργία της εκάστοτε εφαρμογής. Τα στοιχεία αυτά μπορεί να είναι το οτιδήποτε, ακόμα και κωδικοί που έχουμε χρησιμοποιήσει στο σύστημά μας.

Το πιο διαδεδομένο αρχείο swap σε κάθε λειτουργικό σύστημα είναι η εικονική του μνήμη. Είναι στην ουσία ένα στιγμιότυπο της μνήμης RAM, όπου σκοπό του έχει να διατηρήσει την λειτουργία του υπολογιστή όταν εξαντληθεί η φυσική μνήμη, αλλά και να ξεκινήσει γρήγορα το σύστημά μας όταν εκείνο επιστρέφει από κατάσταση hibernation.

- `Apple Menu -> System Preferences -> Accounts`
- `Select your username -> Select the Password field`
- `If asked, type in your current password -> Type in a new password -> verify the new password`



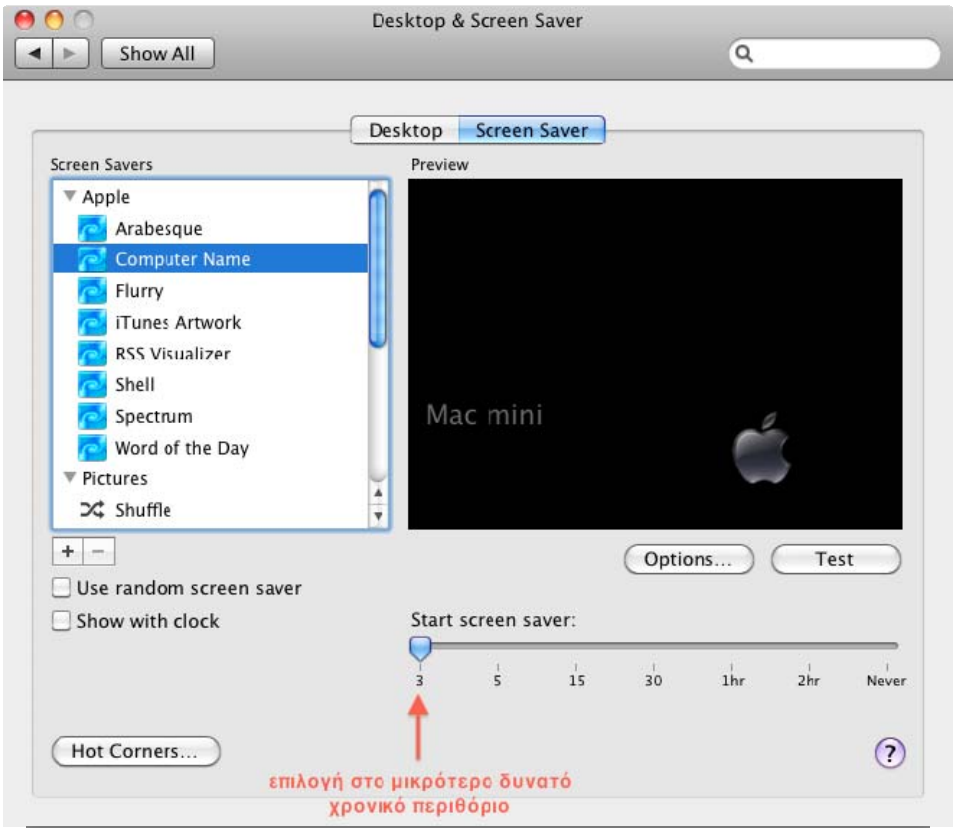
Εικόνα 12 - Παράθυρο αλλαγής κωδικού χρήστη

[11] http://en.wikipedia.org/wiki/Virtual_memory

2.1.3. Προφύλαξη οθόνης

Το Mac OS X έρχεται με ενσωματωμένη προστασία οθόνης που περιλαμβάνει κλείδωμα με κωδικό. Αυτό καλό θα είναι να παραμένει ενεργό προκειμένου να αποτρέψει κάποιον από το να αποκτήσει χρήση του υπολογιστή όταν εσείς απομακρυνθείτε από αυτόν. Για να ενεργοποιήσουμε την προστασία οθόνης :

- Apple menu -> System Preferences -> Desktop & Screensaver -> Screen Saver -> (Select a screen-saver)
- Change "Start screen saver" to 3 minutes



Εικόνα 13 – Επιλογές ScreenSaver

Για να ενσωματώσουμε κωδικό στην προστασία οθόνης :

- Apple -> System Preferences -> Security
- Check "Require password to wake this computer from sleep or screen saver"

Εικόνα 14 –Παράθυρο Ρυθμίσεων Ασφάλειας

Μπορεί να θέλετε μία ενεργή γωνία στην επιφάνεια εργασίας, προκειμένου να απενεργοποιήσουμε την έναρξη της προστασίας οθόνης ύστερα από ένα χρονικό διάστημα αδράνειας (αυτό μπορεί να είναι χρήσιμο όταν βλέπουμε μια ταινία) και , ακόμα σημαντικότερο, μπορούμε να ενεργοποιήσουμε χειροκίνητα την προστασία οθόνης :

- Apple menu -> System Preferences -> Desktop & Screensaver -> Screen Saver -> Hot Corners
- Choose a corner, e.g. bottom right -> Disable Screen Saver
- Choose a corner, e.g. top right -> Start Screen Saver

Εικόνα 15 – Παράθυρο Επιλογής Hot Corners

2.2. Ρύθμιση POSIX, ACL και άδειες εισόδου

Τα δεδομένα μας είναι το σημαντικότερο σημείο του υπολογιστή μας. Με την χρήση κωδικοποίησης μπορούμε να τα προστατέψουμε στην περίπτωση επίθεσης ή κλοπής του υπολογιστή μας.

Ρυθμίζοντας γενικές συνθήκες προσβασιμότητας, κωδικοποιώντας βασικούς φακέλους χρήστη και δεδομένων, μπορούμε να είμαστε σίγουροι ότι τα δεδομένα μας είναι ασφαλή. Επιπλέον, με τα εργαλεία που μας παρέχονται στο Mac OSX , μπορούμε να κάνουμε πλήρη και ασφαλή διαγραφή των δεδομένων μας.

2.2.1. Κατανοώντας τους κανόνες πρόσβασης

Προστατεύουμε τα αρχεία μας και τους φακέλους δημιουργώντας κανόνες πρόσβασης που επιτρέπουν ή απαγορεύουν πρόσβαση σε αυτά. Το Mac OS X υποστηρίζει δύο τρόπους ρύθμισης κανόνων πρόσβασης :

- Το POSIX[12] που είναι καθιερωμένο στο UNIX.

[12] Portable Operating System Interface

- Τα ACLs[13].Χρησιμοποιούνται από το Mac OSX και είναι συμβατά με τα Microsoft Windows Server 2003 και Microsoft Windows XP.

Το ACL χρησιμοποιεί POSIX όταν κάνει επαλήθευση στις άδειες πρόσβασης των αρχείων και φακέλων. Η διαδικασία του χρησιμοποιεί το πρωτόκολλο ACL για να επιβεβαιώσει ότι μία εγγραφή επιτρέπεται ή απαγορεύεται περιλαμβάνει κανόνες επαλήθευσης που ονομάζονται ACEs (access control entries). Αν κανένα ACEs δεν μπορεί να εφαρμοστεί, τότε οι καθιερωμένοι POSIX κανόνες ρυθμίζουν την πρόσβαση.

[13] Access Control Lists

2.2.2. Ρυθμίσεις των κανόνων πρόσβασης POSIX

Το Mac OS X βασίζει τους κανόνες πρόσβασης των αρχείων του στο πρωτόκολλο POSIX. Αυτό περιλαμβάνει τους κανόνες εγγραφής, ιδιοκτησίας του αρχείου και της πρόσβασης. Κάθε αρχείο και φάκελος έχει τους τρεις κανόνες πρόσβασης, ανάγνωση, εγγραφή και εκτέλεση (read, write, execute), όπου εφαρμόζονται στις τρεις κατηγορίες χρηστών, ιδιοκτήτης, ομάδα και οποιοσδήποτε (user, group, everyone). Μπορούμε να εφαρμόσουμε τέσσερεις κανόνες πρόσβασης POSIX σε κάθε αρχείο ή φάκελο : Εγγραφή και Ανάγνωση (Read and Write), Εγγραφή μόνο (Write Only), Ανάγνωση μόνο (Read Only) και Καμία (None).

2.2.3. Παρακολούθηση των κανόνων πρόσβασης POSIX

Μπορούμε να εφαρμόσουμε προρυθμισμένους κανόνες πρόσβασης POSIX στις παρακάτω κατηγορίες χρηστών :

Ιδιοκτήτης (Owner)-Ο χρήστης που δημιουργεί ένα αρχείο ή φάκελο στον υπολογιστή και έχει δικαιώματα Ανάγνωσης και Εγγραφής (Read and Write) για αυτό το αρχείο ή φάκελο. Ως προεπιλογή ο ιδιοκτήτης ενός αρχείου ή φακέλου η ο διαχειριστής του συστήματος μπορούν να αλλάξουν τις ρυθμίσεις πρόσβασης (να επιτρέψουν μία νέα ομάδα να έχει πρόσβαση ή ακόμα και ο οποιοσδήποτε να το χρησιμοποιήσει). Ο διαχειριστής μπορεί επίσης να μεταφέρει ιδιοκτησία και σε κάποιον άλλο χρήστη.

Ομάδα (Group) - Μπορούμε να αναθέσουμε χρήστες που χρειάζονται παρόμοια πρόσβαση σε αρχεία και φακέλους σε έναν λογαριασμό ομάδας. Μόνο σε μία ομάδα μπορεί να ανατεθεί πρόσβαση σε ένα κοινόχρηστο αντικείμενο.

Οποιοσδήποτε (Everyone) - Αυτοί μπορεί να είναι οποιοδήποτε χρήστες που μπορούν να βρίσκονται στο σύστημα (εγγεγραμμένοι ή μη).

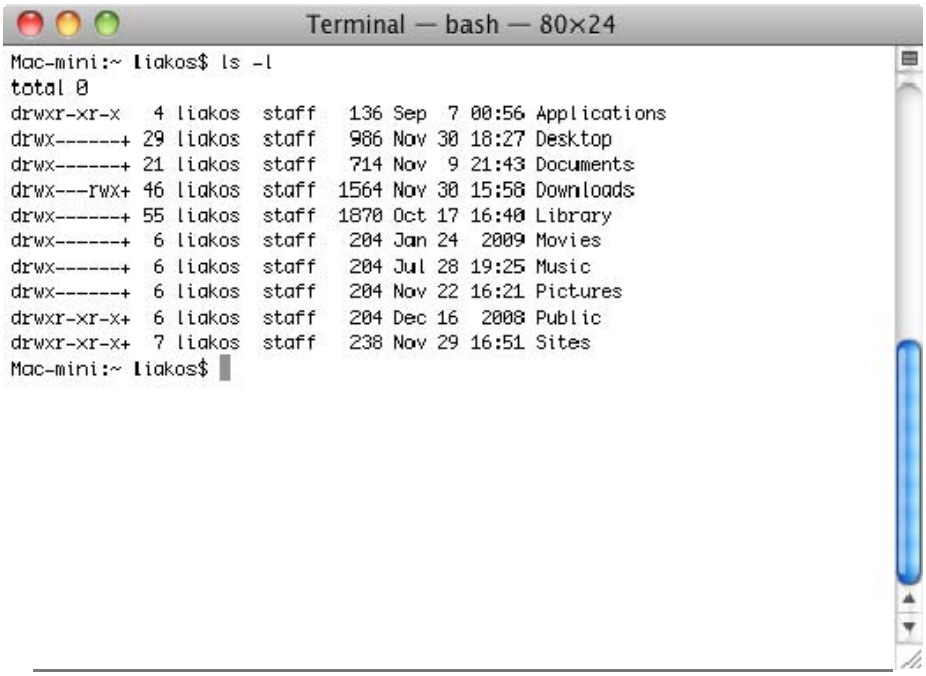
Πριν ρυθμίσουμε ή αλλάξουμε τις τιμές πρόσβασης του POSIX, πρέπει να δούμε τις τωρινές ρυθμίσεις. Για να δούμε τις τιμές φακέλων ή αρχείων :

1. Ανοίγουμε την εφαρμογή Terminal.

2. Από την γραμμή εντολών εκτελούμε την `ls`:

```
$ ls -l
```

Εμφανίζεται κάτι σαν το παρακάτω :

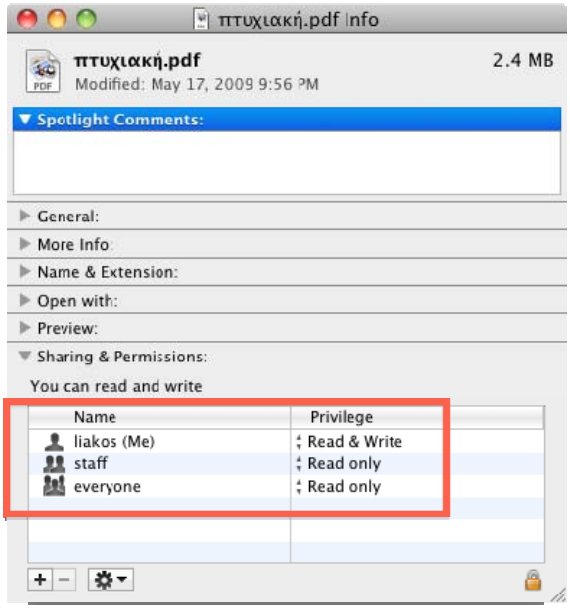


Εικόνα 16 - Περιεχόμενα home directory

Σημείωση : Το '~' αναφέρεται στο home φάκελο του εκάστοτε χρήστη, που στην συγκεκριμένη περίπτωση είναι /Users/liakos.

~/Documents/ είναι ο φάκελος εργασίας.

Μπορούμε επίσης και μέσω του Finder να ελέγξουμε τις τιμές του POSIX. Μέσα από τον Finder επιλέγουμε ένα αρχείο, πατάμε Control-Click και στην συνέχεια επιλέγουμε Get Info. Μετά Ownership & Permissions όπου μέσα από το μενού μπορούμε να δούμε τις τιμές POSIX.



Εικόνα 17 - Ownership & Permissions Info

2.2.4. Ερμηνεία των τιμών πρόσβασης του συστήματος POSIX

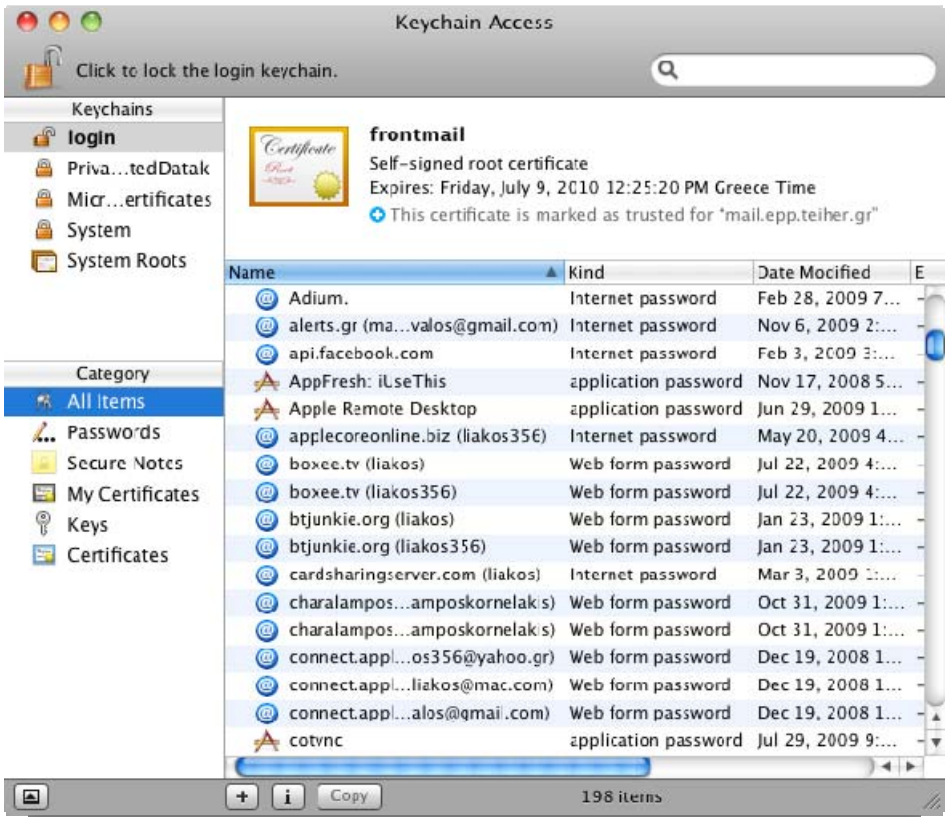
Για να ερμηνεύσουμε τις τιμές POSIX, διαβάζουμε τα πρώτα 10 ψηφία της λίστας αρχείων

- `drwxr-xr-x 2 liakos liakos 68 Apr 28 2006 NewFolder`

Στο παραπάνω παράδειγμα, το NewFolder έχει τιμές POSIX drwxr-xr-x και έχει έναν ιδιοκτήτη και ομάδα με το όνομα liakos.

2.3. Keychain -Κλειδούχος

Στο Mac OS X περιλαμβάνεται ένα πρόγραμμα που αποθηκεύει τους κωδικούς που χρησιμοποιούνται συχνά. Πρέπει να σημειωθεί ότι πάντα περιλαμβάνεται ένα ρίσκο όσον αφορά την αποθήκευση κωδικών στον υπολογιστή, ασχέτως από το λογισμικό που χρησιμοποιούμε.



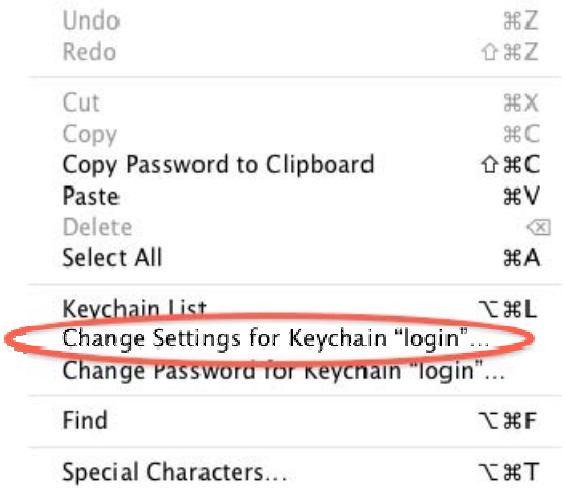
Εικόνα 18 - Κεντρικό παράθυρο Keychain

Το πρόγραμμα Keychain-Κλειδούχος αποθηκεύει τους κωδικούς σε κωδικοποιημένη μορφή και είναι δύσκολο για έναν χρήστη που δεν είναι

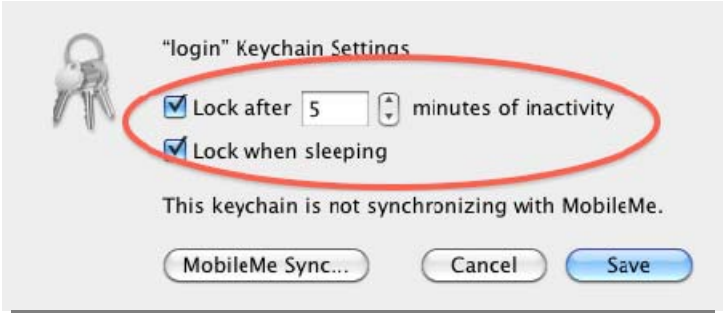
διαχειριστής να ανακτήσει αυτούς τους κωδικούς από τις εφαρμογές που χρησιμοποιούνται. Παρόλα αυτά, παρόμοια με το παράθυρο εκκίνησης , είναι πιθανό κάποιος με δικαιώματα διαχειριστή να ανακτήσει τον κωδικό ενός χρήστη που χρησιμοποιεί στον Κλειδούχο. Η ασφαλέστερη μέθοδος είναι να θυμόσαστε τους κωδικούς σας δίχως να τους αποθηκεύετε στον υπολογιστή.

Υπάρχει ένα πλήθος από βήματα που μπορεί κάποιος να κάνει ώστε να ελαχιστοποιήσει το ενδεχόμενο χαμένων κωδικών όταν είναι σε χρήση ο Κλειδούχος. Προκειμένου να ενεργοποιήσουμε το αυτόματο κλείδωμα του Κλειδούχου :

- Applications -> Utilities -> Keychain Access -> Edit -> Change settings for Keychain "login"
- Check "Lock after"
- Change "minutes of inactivity" to 5 minutes
- Check "Lock when sleeping"
- Save



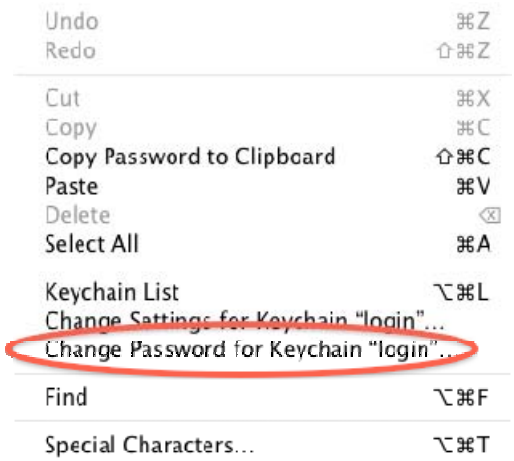
Εικόνα 19 – Menu Edit κλειδούχου



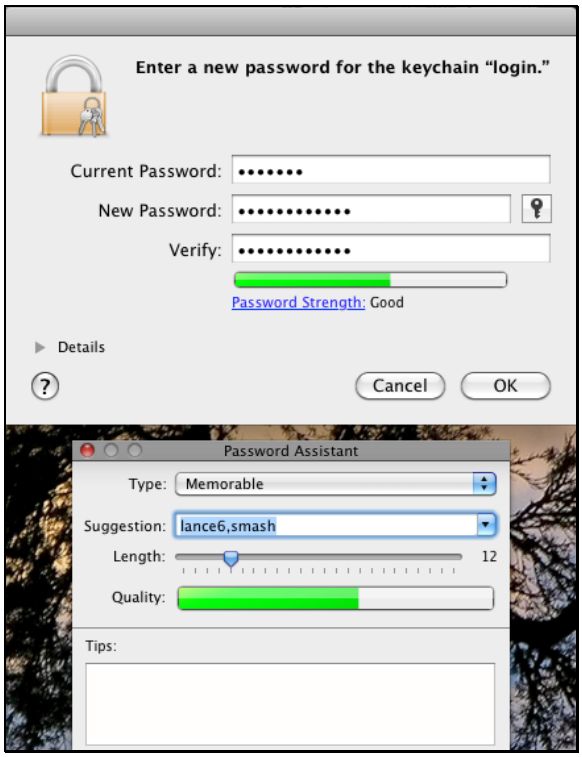
Εικόνα 20 – Επιλογές κλειδώματος

Ως προεπιλογή, το Mac OS X χρησιμοποιεί τον ίδιο κωδικό για τον κλειδούχο και για την εισαγωγή σας στο σύστημα. Μία καλή συμβουλή είναι να κρατούμε αυτούς τους δύο κωδικούς διαφορετικούς :

- Edit -> Change Password for Keychain "login"
- Type in your current user's login password
- Type in a new different password twice
- OK



Εικόνα 21 - Menu Edit κλειδούχου



Εικόνα 22 - Παράθυρο Αλλαγής Κωδικού Κλειδούχου

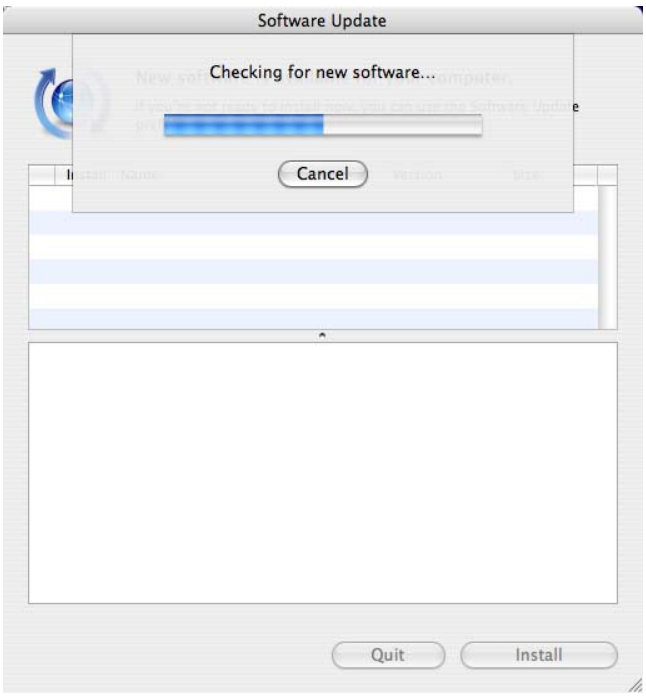
2.4. Patching-Ενημερώσεις λειτουργικού

Όπως συνήθως συμβαίνει, θα πρέπει να κρατάτε το Mac OS X λειτουργικό συνέχεια ενημερωμένο με τις τελευταίες ρυθμίσεις, όπου συχνά περιλαμβάνουν διορθώσεις στο τομέα της ασφάλειας.

2.4.1. Apple Software Update (το επίσημο εργαλείο ενημέρωσης)

Το OS X περιλαμβάνει ένα εργαλείο που είναι υπεύθυνο για τις περισσότερες ενημερώσεις των εφαρμογών της Apple. Το Software Update συχνά περιλαμβάνει σημαντικές αναβαθμίσεις ασφάλειας που πρέπει να ενσωματωθούν στο λειτουργικό μας σύστημα. Η εφαρμογή αυτόματα ελέγχει για ποιες ενημερώσεις είναι διαθέσιμες και αν υπάρχουν σημαντικές αλλαγές στο σύστημα, μπορεί να κατεβάσει μόνο τα στοιχεία που απαιτούνται και όχι ολόκληρες τις εφαρμογές.

Είναι καλύτερο να ρυθμίζεις το Software Update για αυτόματο έλεγχο των ενημερώσεων σε τακτά χρονικά διαστήματα :



Εικόνα 23 - Παράθυρο Αναβαθμίσεων

- Apple Menu -> System Preferences -> Software Updates
- Check "Check for updates"
- Choose "Daily" from drop-down menu.

Εικόνα 24 - Επιλογές αυτόματης ενημέρωσης λειτουργικού

Το μηχάνημά σας θα ελέγχει για ενημερώσεις λογισμικού μια φορά την ημέρα και θα σας υπενθυμίζει πότε υπάρχουν καινούργιες έτοιμες για download.

Το Software update μπορεί να εκτελεστεί και από την γραμμή εντολών αν έχουμε λογαριασμό διαχειριστή :

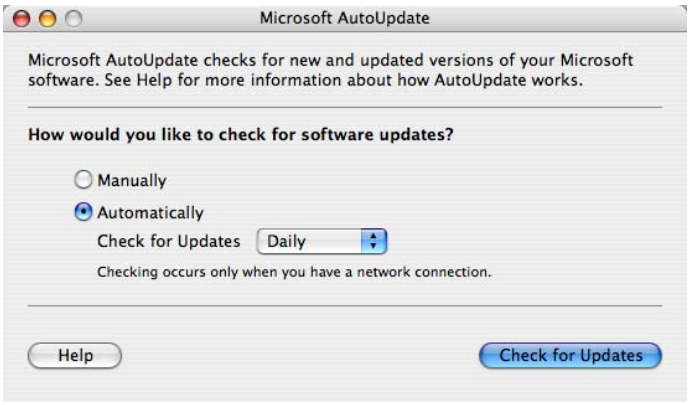
```
• /usr/sbin/softwareupdate -ia
```

Και να προγραμματιστεί να εκτελείται :

```
• /usr/sbin/softwareupdate -schedule on
```

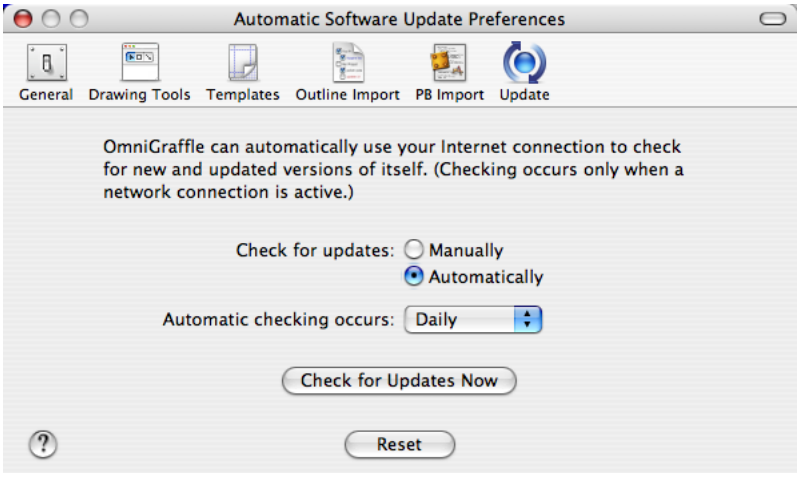
2.4.2. Λοιπές Ενημερώσεις

Αρκετές λοιπές εφαρμογές, πέρα από εκείνες που έχουν κατασκευαστεί από την Apple, μπορεί να έχουν το δικό τους εργαλείο για έλεγχο νέων εκδόσεων. Ένα παράδειγμα είναι το Microsoft AutoUpdate:



Εικόνα 25 - Παράθυρο Αναβαθμίσεων Τρίτων Εφαρμογών

Άλλα προγράμματα, όπως το OmniGraffle, περιλαμβάνουν την διαδικασία αυτόματης αναβάθμισης από το ίδιο το πρόγραμμα :

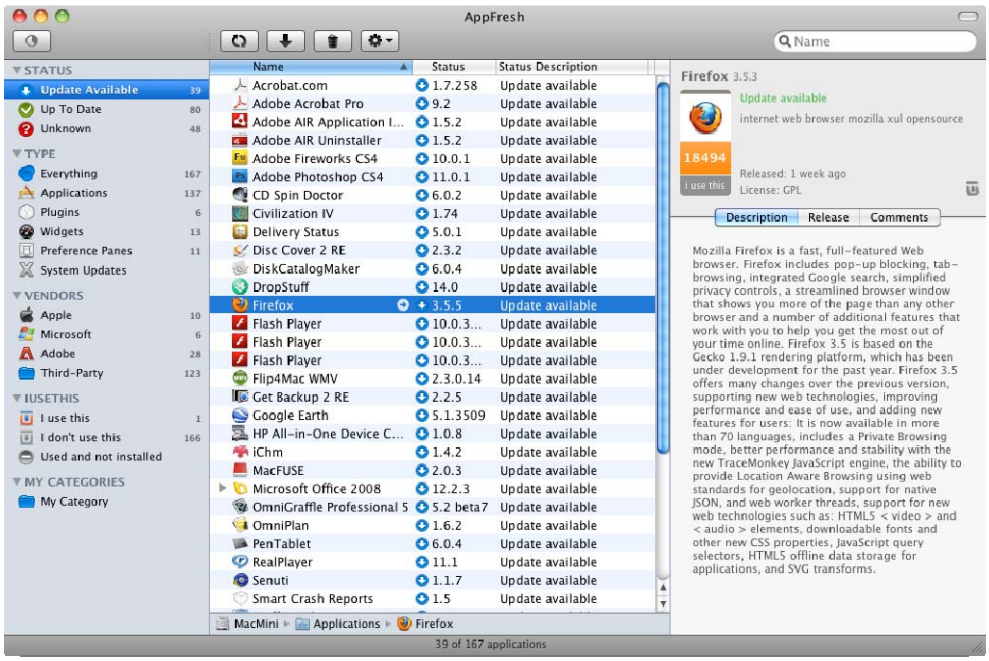


Εικόνα 26 - Παράθυρο Αναβαθμίσεων Λοιπών Εφαρμογών

Είναι πολύ καλή πρακτική να ενημερώνουμε όσα προγράμματα έχουμε με όλες τις διαθέσιμες αναβαθμίσεις, προκειμένου να προλαμβάνουμε τυχών κενά ασφαλείας που παρουσιάζονται κατά την χρήση τους.

2.4.3. Αναβαθμίσεις μέσω Appfresh

Πρόσφατα παρουσιάστηκε για το OS X η δωρεάν εφαρμογή Appfresh[14], όπου μας επιτρέπει να κάνουμε ένα συνολικό έλεγχο στο σύστημά μας και να αναβαθμίσουμε συνολικά όλο το σύστημά μας. Αυτό μπορεί να περιλαμβάνει διορθώσεις λογισμικού από την ίδια την Apple αλλά και εφαρμογές από τρίτους κατασκευαστές.

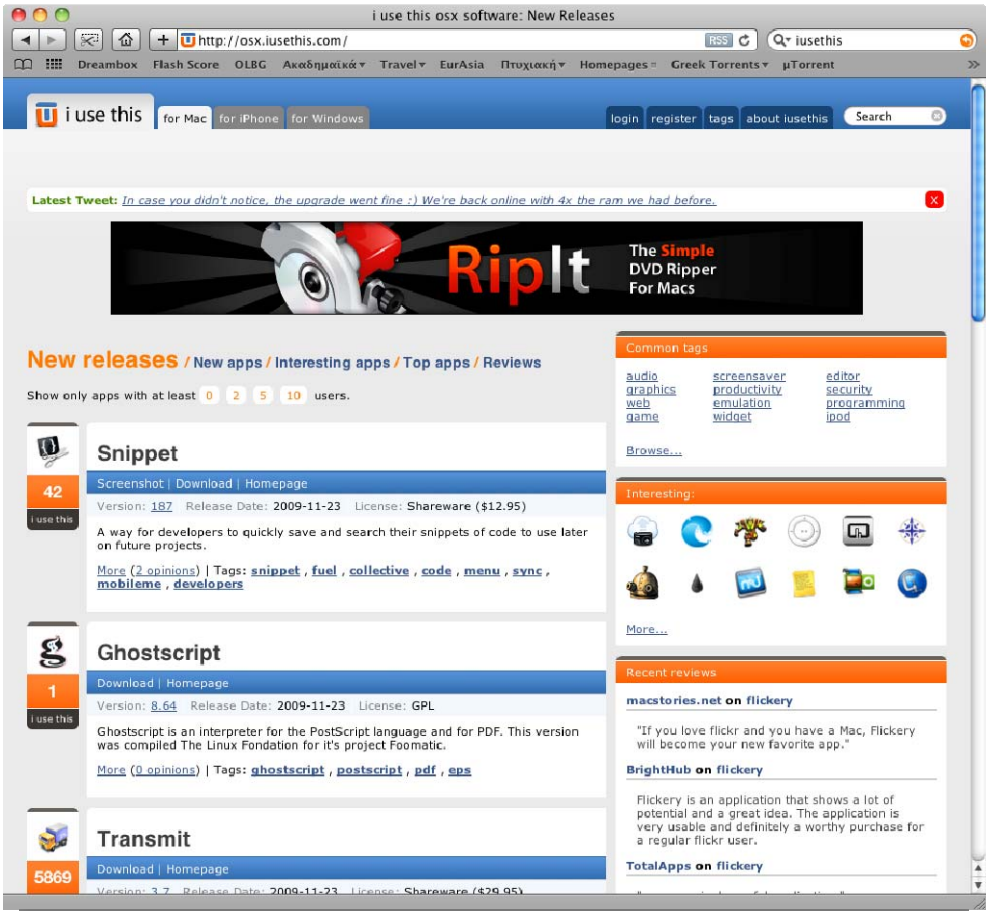


Εικόνα 27 - Κεντρικό παράθυρο εφαρμογής Appfresh

Αυτό το επιτυγχάνει λαμβάνοντας δεδομένα από το Apple update αλλά και ελέγχοντας όλες τις εκδόσεις των προγραμμάτων που υπάρχουν εγκατεστημένα και στη συνέχεια συγκρίνοντας αυτές τις εκδόσεις, με τις αναβαθμισμένες στον κεντρικό server της εφαρμογής. Σε περίπτωση που βρεθεί κάποια εφαρμογή που δεν είναι καταχωρισμένη στο server του προγράμματος, τότε μπορεί να αντλήσει

[14] http://metaquark.de/appfresh/

πληροφορίες από την community based βάση δεδομένων iUseThis.com[15]. Το παραπάνω είναι ένα site που ενημερώνεται από τους ίδιους τους χρήστες για κάθε πιθανή εφαρμογή που μπορεί να κυκλοφορεί διαθέσιμο για mac.



Εικόνα 28 - iUseThis site για αναβαθμίσεις εφαρμογών

2.5. Κωδικοποίηση δεδομένων

Υπάρχουν αρκετές μέθοδοι για να κωδικοποιήσουμε τα δεδομένα μας στο OS X. Μακράν η ασφαλέστερη είναι με την χρήση του GnuPG[16], παρόλα αυτά, η εφαρμογή FileVault της Apple και η χρήση εικονικών δίσκων, είναι πιο βολική.

2.5.1. FileVault και κωδικοποιημένοι εικονικοί δίσκοι

Το FileVault της Apple είναι μία χρήση των κωδικοποιημένων εικονικών δίσκων με την χρήση του αλγορίθμου AES, όπου προσαρτώνται αυτόματα ως home directory όταν κάνετε login στο σύστημα και κωδικοποιεί/αποκωδικοποιεί

[15] http://osx.iusethis.com/

[16] http://www.gnupg.org/

δεδομένα σε πραγματικό χρόνο. Η κωδικοποίηση δεδομένων στο δίσκο δεν είναι κάτι καινούργιο, αλλά η Apple από την έκδοση 10.3 του OS X παρουσίασε το πρώτο UNIX λειτουργικό σύστημα που περιλαμβάνει αυτή την δυνατότητα εγγενώς. Όταν λειτουργεί το FileVault, ο χρήστης δεν αντιλαμβάνεται ότι πραγματοποιείται κάποια κωδικοποίηση, παρά μόνο μία μικρή ως αμελητέα μείωση της απόδοσης.

Για την ενεργοποίηση του FileVault:

- `Apple menu -> System Preferences -> Security`
- `Turn on FileVault`

Εικόνα 29 - Επιλογές παραθύρου ασφάλειας

Ανάλογα με το μέγεθος που προσωπικού σας φακέλου (home directory), απαιτείται και ο ανάλογος χρόνος για την κωδικοποίησή του από το FileVault. Θα πρέπει να σημειωθεί ότι μετά την κωδικοποίηση των δεδομένων σας, αυτά δεν έχουν διαγραφεί με ασφάλεια. Απλά έχει περιοριστεί η πρόσβαση σε αυτά και ως αποτέλεσμα, μπορούν να ανακτηθούν.

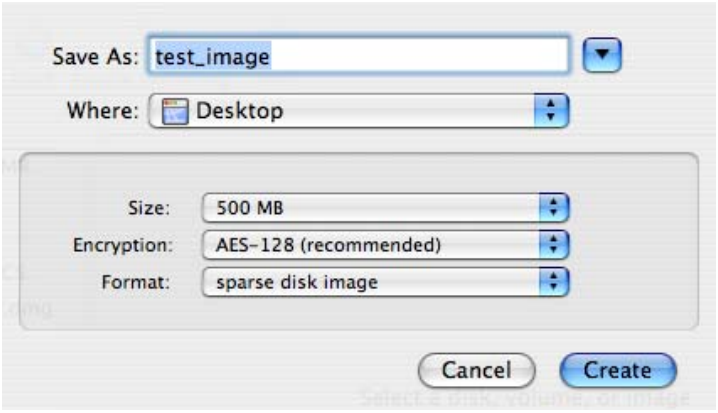
Μπορεί επίσης να θέλετε να ορίσετε έναν βασικό κωδικό για τον υπολογιστή. Ο βασικός κωδικός θα πρέπει να είναι διαφορετικός από τον κωδικό χρήστη (άρα και από τον κωδικό του FileVault), και θα πρέπει να χρησιμοποιείται για αποκωδικοποίηση των δεδομένων του FileVault σε περίπτωση χαμένου κωδικού.

Από την πλευρά της εξασφάλισης του συστήματος, να υπενθυμίσουμε ότι κάποιος με φυσική πρόσβαση στον υπολογιστή ή με λογαριασμό διαχειριστή μπορεί να αποκτήσει πρόσβαση στον δικό σας κωδικό του FileVault και να έχει πρόσβαση στα προσωπικά σας δεδομένα.

2.5.2. Κωδικοποιημένοι εικονικοί δίσκοι με την χρήση AES

Οι κωδικοποιημένοι εικονικοί δίσκοι της Apple δεν προσφέρουν την ίδια ευκολία στην χρήση με το FileVault, αλλά παρόλα αυτά κωδικοποιούν σε πραγματικό χρόνο όταν κάνεις καταχώρηση πάνω σε αυτούς. Για να δημιουργήσετε έναν κωδικοποιημένο εικονικό δίσκο :

- Applications -> Utilities -> Disk Utility
- New Image
- Save as -> Choose a name for the file system and image file name
- Where -> Choose a location to save the image file
- Size -> Choose a maximum size to allow the image to grow to
- Encryption -> Choose AES-128
- Format -> Sparse Disk Image
- Create -> Enter and Verify password
- Check or uncheck "Remember password (add to Keychain)



Εικόνα 30 – Παράθυρο Αποθήκευσης Κωδικοποιημένων Εικονικών Δίσκων

Μόλις δημιουργήσετε τον κωδικοποιημένο εικονικό δίσκο, μπορείτε να τον προσαρτήσετε με διπλό κλικ, και εκείνος θα εμφανιστεί στην διαχείριση των αρχείων. Η τοποθεσία του θα είναι /Volumes/<image file system name> και ένα εικονίδιο θα εμφανιστεί στην επιφάνεια εργασίας.

2.5.3. Αδυναμίες FileVault

Ένα βασικό μειονέκτημα του FileVault είναι ότι δεν μπορούμε να επιλέξουμε συγκεκριμένα μέρη από τον σκληρό μας δίσκο για κωδικοποίηση. Μόνο ολόκληρα home directories μπορούνε να επιλεχθούν για κωδικοποίηση. Για παράδειγμα, με την χρήση του FileVault δεν μπορούμε να κωδικοποιήσουμε όλο τον σκληρό δίσκο, κάτι που μπορεί να γίνει με άλλα προγράμματα όπως το as PGP[17] Whole Disk Encryption. Παρόμοια, μεμονωμένα αρχεία και φάκελοι δεν μπορούν να επιλεχθούν ξεχωριστά για την κωδικοποίηση του FileVault.

Κριτική έχει λάβει και ο τρόπος κρυπτογράφησης του FileVault. Παρότι προβάλλεται ως "128-bit AES encryption", η κωδικοποίησή του μπορεί να σπάσει με την χρήση 1024-bit RSA[18] ή 3DESEDE[19], όπου και τα δύο θεωρούνται περισσότερο αδύναμα σε σχέση με το 128-bit AES. Επίσης προβληματική θεωρείται και η χρήση του CBC[20] mode of operation και η επισφαλής αποθήκευση κλειδιών στη swap memory ύστερα από sleep mode[21].

Επίσης, λογαριασμοί που έχουν ενεργοποιημένο το FileVault μπορούν να ενσωματωθούν σε έναν νέο Mac υπολογιστή μόνο αν το νέο σύστημα δεν έχει ενεργούς λογαριασμούς χρηστών, διαφορετικά η προστασία που προσφέρει το FileVault πρέπει να απενεργοποιηθεί κατά την ενσωμάτωση ή το λειτουργικό σύστημα να εγκατασταθεί εξ' αρχής.

Μια πολύ ενδιαφέρουσα έκθεση[22] που παρουσιάστηκε το 2008, έδειξε ένα σημαντικό κενό στις μνήμες που χρησιμοποιούν οι υπολογιστές μας. Το φαινόμενο των «υπολειμμάτων δεδομένων» ή data remanence[23] στις μνήμες DRAM είναι ο χρόνος που απαιτείται για να εκφορτιστεί και να καθαριστεί ένα DIMM μνήμης από τα δεδομένα του. Αυτή η μελέτη έδειξε ότι απαιτούνται αρκετά δευτερόλεπτα ως λεπτά για να καθαριστεί ένα DIMM RAM και αυτός ο χρόνος αυξάνεται ακόμα περισσότερο αν βρισκόμαστε σε ψυχρό περιβάλλον. Με βάση αυτό το φαινόμενο και με την μέθοδο του cold boot attack[24], μπορεί κάποιος να ανακτήσει κρυπτογραφημένα κλειδιά από διάφορα συστήματα ασφαλείας, ένα

[17] http://www.pgp.com/

[18] http://en.wikipedia.org/wiki/RSA

[19] http://en.wikipedia.org/wiki/3DES-EDE

[20] Block cipher modes of operation - http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation

[21] http://en.wikipedia.org/wiki/Sleep_mode

[22] Lest We Remember: Cold Boot Attacks on Encryption Keys - http://citp.princeton.edu.nyud.net/pub/coldboot.pdf

[23] http://en.wikipedia.org/wiki/Data_remanence

[24] http://en.wikipedia.org/wiki/Cold_boot_attack

από τα οποία είναι και το FileVault, εκμεταλλευόμενος τον τρόπο με τον οποίο τα κλειδιά αποθηκεύονται στη μνήμη ύστερα από μία επιτυχή αναγνώριση. Το συμπέρασμα της μελέτης ήταν ότι οι χρήστες είναι προτιμότερο να σβήνουν φυσικά τον υπολογιστή τους, από να τον αφήνουν σε κατάσταση sleep.

2.5.4. Openssl και κωδικοποιημένα αρχεία

Μία εναλλακτική λύση, είναι η χρήση του openssl και ενός κωδικού για να ασφαλίσουμε ένα αρχείο. Το Openssl link δεν χρησιμοποιεί ασύμμετρα κλειδιά (π.χ. Ιδιωτικό και δημόσιο κλειδί) και επιτρέπει απλά την χρήση ενός κωδικού σε ένα αρχείο. Παρόλα αυτά, το openssl στο OS X μπορεί να υποφέρει από τις αδυναμίες που υποφέρει και το FileVault.

Για να κωδικοποιήσετε ένα αρχείο με την χρήση του openssl και τον αλγόριθμο blowfish των 128bit :

```
• openssl bf -salt -in <plain file> -out <encrypted
  file>
```

Ύστερα εφαρμόζουμε πλήρη διαγραφή (γέμισμα με μηδενικά) στα αρχικά δεδομένα :

```
• srm -fm <input file>
```

Τέλος, για επαναφορά του αρχείου :

```
• openssl bf -d -in <encrypted file> -out <plain
  file>
```

Ένα script για να κωδικοποιήσουμε έναν ολόκληρο φάκελο more exhghsh :

```
• #!/bin/sh
• #
• # Script to encrypt a dir and securely remove it.
• if [ $# -lt 1 ] ; then
• echo "Usage: $0 dir_to_encrypt"
• exit 1
• fi
• file=`echo $1 | sed s/"\/"//g | sed s/"\."//g`
• dir=$1
• echo -n "Checking if $dir actually exists... "
• if [ -d $dir ] ; then
• echo "Yes."
• else
• echo "No. Exiting."
```

```
• exit 1
• fi
• echo -n "Checking to make sure $file.tar.gz.bf
  doesn't already exist... "
• if [ -e $file.tar.gz.bf ] ; then
• # exists
• echo "Yes. Exiting."
• exit 1
• else
• # doesn't exist
• echo "No."
• fi
• echo -n "Checking to make sure tempfile doesn't
  already exist... "
• if [ -e temp.tar.gz ] ; then
• echo "Yes. Exiting. You need to remove
  temp.tar.gz."
• exit 1
• else
• echo "No."
• fi
• echo "Tarring up directory..."
• tar -zcvf temp.tar.gz $dir
• echo "Done."
• echo "Encrypting directory..."
• openssl bf -salt -in temp.tar.gz -out
  $file.tar.gz.bf
• echo "Done."
• echo
• echo "Here is what the encrypted archive looks
  like:"
• ls -l $file.tar.gz.bf
• echo
• echo "Is it safe to securely remove $dir? (y)/n"
• read remove
• if [ x$remove = xn ] || [ x$remove = xN ]; then
• echo "Ok, exiting without removing it."
• srm -fm temp.tar.gz
• exit 0
• else
• echo "Ok, removing $dir securely and exiting..."
• srm -rfm $dir
• srm -fm temp.tar.gz
• echo "Done"
```

```
fi
exit
```

Τέλος, ένα παρόμοιο script για να αποκωδικοποιήσουμε έναν φάκελο πίσω στην αρχική του μορφή :

```
#!/bin/sh
#
# Script to decrypt a tar.gz.bf archive
if [ $# -lt 1 ] ; then
echo "Usage: $0 archive_to_decrypt"
exit 1
fi
file=$1
dir=`echo $1 | cut -d "." -f 1`
echo -n "Checking if $file actually exists... "
if [ -f $file ] ; then
echo "Yes."
else
echo "No. Exiting."
exit 1
fi
echo -n "Checking to make sure $dir doesn't already exist... "
if [ -f $dir ] ; then
# exists
echo "Yes. Exiting."
exit 1
else
# doesn't exist
echo "No."
fi
echo -n "Checking to make sure tempfile doesn't already exist... "
if [ -e temp.tar.gz ] ; then
echo "Yes. Exiting. You need to remove temp.tar.gz."
exit 1
else
echo "No."
fi
echo "Decrypting..."
openssl bf -salt -d -in $file -out temp.tar.gz
echo "Untarring..."
```

```
• tar -zxvf temp.tar.gz
• echo "Cleaning up..."
• rm temp.tar.gz
• echo "All done."
• echo
• exit
```

2.5.5. Κωδικοποίηση αρχείων με την χρήση GnuPG [25]

Το Gnu Privacy Guard (μία έκδοση του PGP υπό την μορφή λογισμικού ανοιχτού κώδικα), σας επιτρέπει να κωδικοποιήσετε τα αρχεία σας με την χρήση δημοσίου κλειδιού. Στην συνέχεια θα μπορείτε να αποκωδικοποιήσετε τα δεδομένα σας με την χρήση ιδιωτικού κλειδιού και τον αντίστοιχο κωδικό του. Υποθέτουμε ότι έχετε εγκατεστημένο στο σύστημά σας το GnuPG και έχετε δημιουργήσει για λογαριασμό σας ένα ζεύγος ιδιωτικού και δημόσιου κλειδιού. Για να κωδικοποιήσετε ένα αρχείο, θα πρέπει να εκτελέσετε την εντολή :

```
• gpg -r <your key's name> --encrypt-files
  <filename>
```

Αυτή θα παράγει το αρχείο filename.gpg.

Θα πρέπει να κάνετε ασφαλή διαγραφή των αρχικών δεδομένων με την εντολή :

```
• srm –fm <filename>
```

Η εντολή srm επικαλύπτει το αρχείο επτά φορές με τυχαίο περιεχόμενο παραγόμενο από τον αλγόριθμο Gutmann[26] προτού το αποκόψει από το σύστημα αρχείων.

Για να αποκωδικοποιήσουμε το αρχείο :

```
• gpg -r <your key's name> --decrypt-files
  <filename.gpg > filename
```

Η εντολή gpg μπορεί να χρησιμοποιηθεί και με συμμετρική κρυπτογραφία, αρκεί να προσθέσουμε τον τελεστή -c στην σύνταξη.

[25] http://www.gnupg.org/

http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html [26]

2.5.6. Ρυθμίζοντας τον κωδικό του Open Firmware

Αν ρυθμίσετε έναν κωδικό Open Firmware στον Mac, θα απενεργοποιήσει οποιαδήποτε κλειδιά εκκίνησης όταν ο υπολογιστής σας ξεκινά. Αυτό σημαίνει ότι αν κάποιος έχει φυσική πρόσβαση στον υπολογιστή σας, δεν θα μπορεί να τον εκκινήσει.
Ο απλούστερος τρόπος για να θέσετε έναν κωδικο OF , είναι να χρησιμοποιήσετε το σχετικό utility από την Apple, όπου μπορεί να βρεθεί στην διεύθυνση : <http://www.apple.com/downloads/MacOS/apple/openfirmwarepassword.html>.

Η παραπάνω εφαρμογή απαιτεί τον δικό σας κωδικό χρήστη ώστε να εκτελέσει την εντολή nvram προκειμένου να ενεργοποιήσει τον κωδικό OF και στην συνέχεια ζητά έναν κωδικό που θα οριστεί ως κωδικός Open Firmware.

Εικόνα 31 – Παράθυρο Εισαγωγής Κωδικού Open Firmware

Για να ρυθμίσετε τον κωδικό μόνοι σας απευθείας από το OpenFirmware:

```
• <power-button>
• option-apple-o-f
• password
• <enter your password>
• setenv security-mode command
• reset-all
```

Μπορεί να θέλετε να αφαιρέσετε τον κωδικό OpenFirmware όταν δεν μπορείτε να εκκινήσετε τον υπολογιστή σωστά και χρειάζεται επανεγκατάσταση λειτουργικού.

Για να κάνετε κάτι τέτοιο, αφαιρέσετε τον κωδικό απευθείας από το OpenFirmware :

```
• <power-button>
• option-apple-o-f
```

```
• <enter password>
• setenv security-mode=none
• nvramrc
• reset-all
```

Σε περίπτωση ανάγκης, ο κωδικός OpenFirmware μπορεί να αφαιρεθεί εάν αλλάξουμε την ποσότητα μνήμης RAM και στην συνέχεια κάνοντας reset στην μνήμη PRAM τρεις φορές (πιέζοντας και κρατώντας τα πλήκτρα option-apple- p-r κατά την εκκίνηση μέχρι να ακούσετε τον υπολογιστή να επανακινείται τρεις φορές). Η παραπάνω διαδικασία είναι ένα πιθανό κενό ασφάλειας και γι'αυτό το λόγο, ο υπολογιστής σας πρέπει να είναι προστατευμένος και σε επίπεδο hardware.

Θα πρέπει να ξέρετε ότι οποιοσδήποτε έχει πρόσβαση διαχειριστή στον υπολογιστή, μπορεί εύκολα να ανακτήσει τον κωδικό του OpenFirmware. Όπως το OpenBoot της εταιρίας Sun, έτσι και το OpenFirmware, επιλέγει να μην κάνει hash τον κωδικό προτού τον τοποθετήσει στην απροσπέλαστη μνήμη. Ο δεκαεξαδικός κωδικός ASCII μπορεί να εμφανιστεί αν εκτελέσετε την ακόλουθη εντολή με δικαιώματα διαχειριστή :

```
• nvram security-password
```

Στη συνέχεια μπορούμε να τον μετατρέψουμε πάλι σε μορφή ASCII προκειμένου να δούμε τον τρέχον κωδικό OpenFirmware.

2.5.7. Απενεργοποίηση της άμεσης προσπέλασης μνήμης από το πρωτόκολλο FireWire.

Ως προεπιλογή, το πρωτόκολλο FireWire αναθέτει στις συσκευές Firewire (camcorders, photocameras, εξωτερικούς σκληρούς δίσκους) πρόσβαση[27] στην φυσική μνήμη του υπολογιστή που είναι συνδεδεμένοι. Κάτι τέτοιο είναι πιθανό ρίσκο ασφαλείας, καθώς τα περιεχόμενα της μνήμης (όπως κωδικοί και τρέχοντα δεδομένα εργασίας) μπορούν να τραβηχτούν από τον υπολογιστή. Εναλλακτικά, ένας hacker μπορεί να εντοπίσει που είναι στη μνήμη η προστασία οθόνης και να εισάγει ορισμένα τυχαία bytes. Κάτι τέτοιο θα έχει ως αποτέλεσμα την διακοπή λειτουργίας του Screen Saver και ανεπιθύμητη δυνατότητα πρόσβασης του υπολογιστή.

Γενικά, το πρωτόκολλο IEEE 1394[28] (Firewire) εμπεριέχει αρκετά κενά ασφαλείας όπου μπορούν να έχουν μεγάλες συνέπειες για τον υπολογιστή. Ορισμένες από αυτές είναι :

- ανάγνωση τυχαίων τομέων της RAM
- εγγραφή στη RAM του υπολογιστή
- πολλές κακόβουλες πράξεις που μπορεί να προκληθούν από τα παραπάνω κενά. Αυτές μπορούν να είναι όλη η αντιγραφή της RAM, εύρεση κλειδιών ssh, περιεχόμενα εικόνας, παράκαμψη κωδικών και πολλά ακόμα…

Μία συγκεκαλλυμένη παρενέργεια της ενεργοποίησης του κωδικού Open Firmware (που παρουσιάσαμε παραπάνω), είναι ότι έμμεσα απενεργοποιεί την πρόσβαση στη φυσική μνήμη του υπολογιστή για τις FireWire συσκευές μέσω του IOFireWireFamily kernel driver.

Η απενεργοποίηση του FireWire DMA φαίνεται να έχει μικρή επίπτωση στην απόδοση των FireWire συσκευών.

2.5.8. Απενεργοποίηση της εισόδου ενός χρήστη (single-user logins)

Οι αρχικές ρυθμίσεις μίας εγκατάστασης, δίχως κωδικό OpenFirmware (ή προερχόμενη από κωδικό OpenFirmware), μπορεί να ξεκινήσει το σύστημα σε κατάσταση ενός χρήστη, κρατώντας πατημένο το πλήκτρο 'S' κατά την εκκίνηση. Αυτή την ιδιότητα μπορεί να την χρησιμοποιήσει ένας κακόβουλος χρήστης με φυσική πρόσβαση προκειμένου να διαβάσει τα δεδομένα σας, να προσθέσει επιπλέον λογαριασμούς χρηστών ή να αλλάξει τους κωδικούς σας.

Η ακόλουθη ενότητα παρουσιάζει μία μέθοδο που εξασφαλίζει ότι ο χρήστης πρέπει να πληκτρολογήσει έναν κωδικό πριν του παρουσιαστεί ένα περιβάλλον όπου θα μπορεί να λειτουργήσει ως διαχειριστής.

---

[27] http://www.hermann-uwe.de/blog/physical-memory-attacks-via-firewire-dma-part-1-overview-and-mitigation

[28] http://www.1394ta.org/Technology/index.htm

Ως διαχειριστές πληκτρολογείτε :

```
• vi /etc/ttys
• :1,$s/secure/insecure/g
• :wq
```

Για να δημιουργήσετε έναν κωδικό όπου θα τον χρησιμοποιεί ο διαχειριστής όταν προσπαθεί να αποκτήσει έλεγχο σε περιβάλλον ενός χρήστη, χρησιμοποιούμε το openssl:

```
• openssl passwd –salt <xy> <password>
```

Αντικαταστήστε τα <xy> με δύο τυχαία γράμματα όπου θα λειτουργήσουν στο "μαγείρεμα" για την εξαγωγή του hash κωδικού, και το <password> με τον κωδικό που θέλετε να χρησιμοποιείτε για το περιβάλλον ενός χρήστη. Αυτός είναι τελείως αποκομμένος από τον τοπικό κωδικό διαχειριστή, όπου όταν υπάρχει, είναι αποθηκευμένος στην βάση δεδομένων του NetInfo.

Τώρα αντιγράψτε τον hash κωδικό που παράγατε από το openssl, ανοίξτε το αρχείο /etc/master.passwd με έναν επεξεργαστή κειμένου και αντικαταστήστε τους αστερίσκους (*) δίπλα στο "root:" με τον κωδικό hash ώστε το αρχείο να έχει την ακόλουθη μορφή :

```
• nobody:*:-2:-2::0:0:Unprivileged
  User:/var/empty:/usr/bin/false
• root:8d4Gfm/Dhzw6Q:0:0::0:0:System
  Administrator:/var/root:/bin/sh
• daemon:*:1:1::0:0:System
  Services:/var/root:/usr/bin/false
```

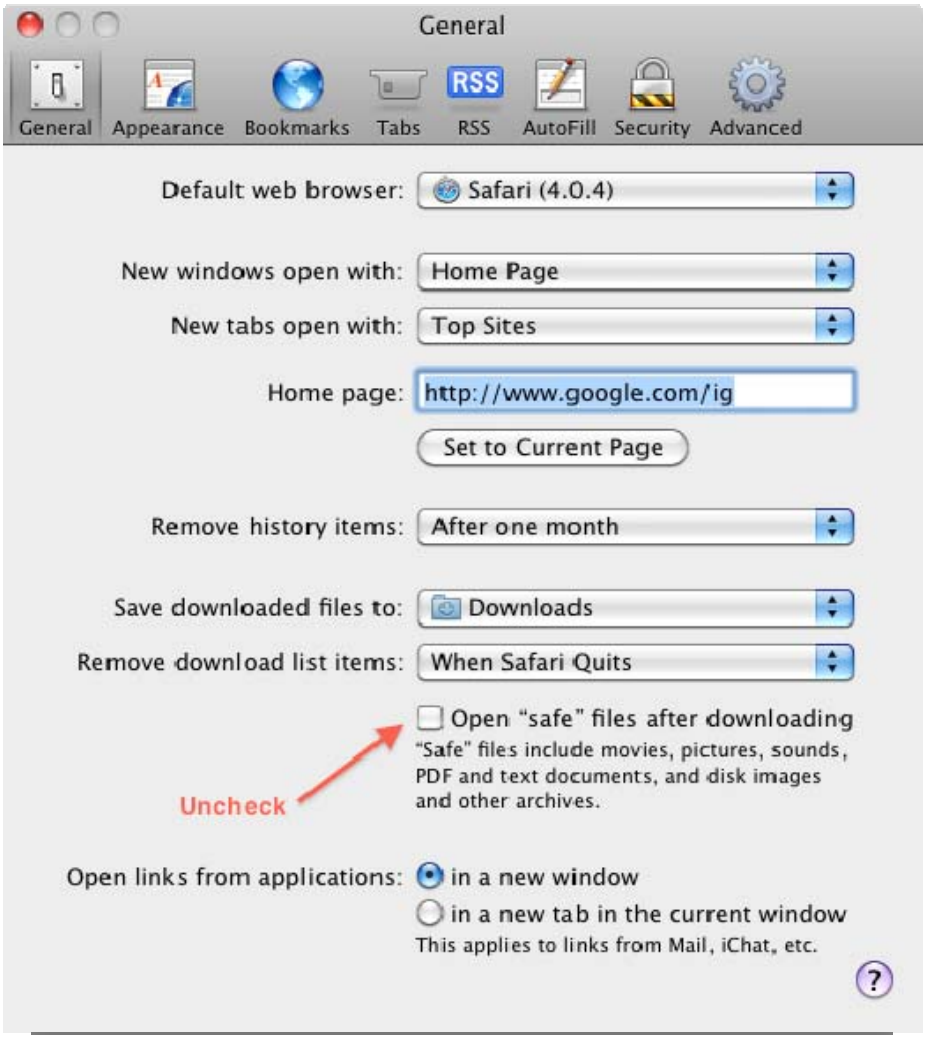
Στην συνέχεια αποθηκεύστε το αρχείο. Από εδώ και στο εξής θα απαιτείται κωδικός για την πρόσβαση σε περιβάλλον ενός χρήστη.

2.5.9. Απενεργοποίηση της αυτόματης έναρξης στον φυλλομετρητή Safari

Ο web browser Safari περιλαμβάνει μία εντολή που του επιτρέπει να εκτελείται το επιλεγμένο πρόγραμμα για κάθε είδος αρχείου. Αυτό μπορεί να αποτελέσει ένα πιθανό κενό ασφάλειας, καθώς ο χρήστης μπορεί άθελά του να εκκινήσει ένα πρόγραμμα παρά την θέλησή του.

Για να απενεργοποιήσουμε αυτό το χαρακτηριστικό :

```
• Safari -> Preferences... -> General
• Uncheck "Open 'safe' files after downloading
```



Εικόνα 32 - Παράθυρο Ρυθμίσεων Safari

2.5.10. Αφαιρώντας άλλους τοπικούς χρήστες

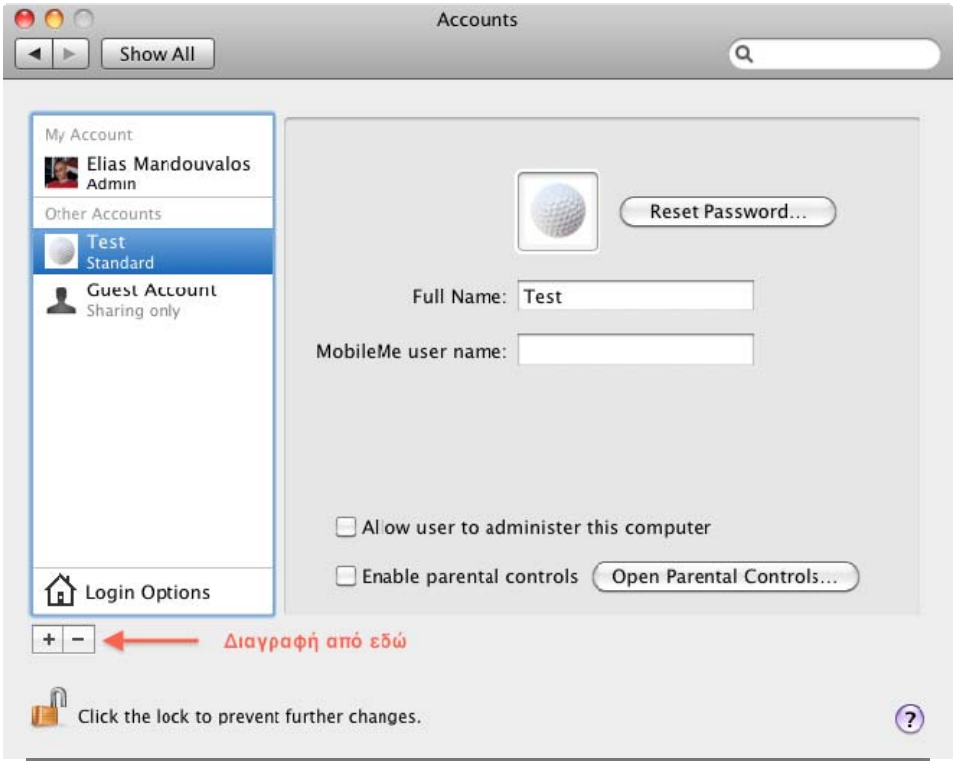
Θα πρέπει να σημειωθεί ότι μία σωστή πρακτική προκειμένου να ασφαλίσουμε περαιτέρω το λειτουργικό μας περιβάλλον, θα πρέπει να μην επιτρέψουμε την πρόσβαση σε άλλους τοπικούς χρήστες, είτε με το Fast User Switching ή το πρωτόκολλο SSH.

2.5.11. Αφαιρώντας τους κανονικούς τοπικούς χρήστες

Ο καλύτερος τρόπος για να αφαιρέσετε έναν περιττό χρήστη είναι μέσω του παραθύρου Accounts System Preferences

- `Apple menu -> System Preferences -> Accounts`
- `Select the other account`

- Click the minus ("-") button -> Delete Immediately

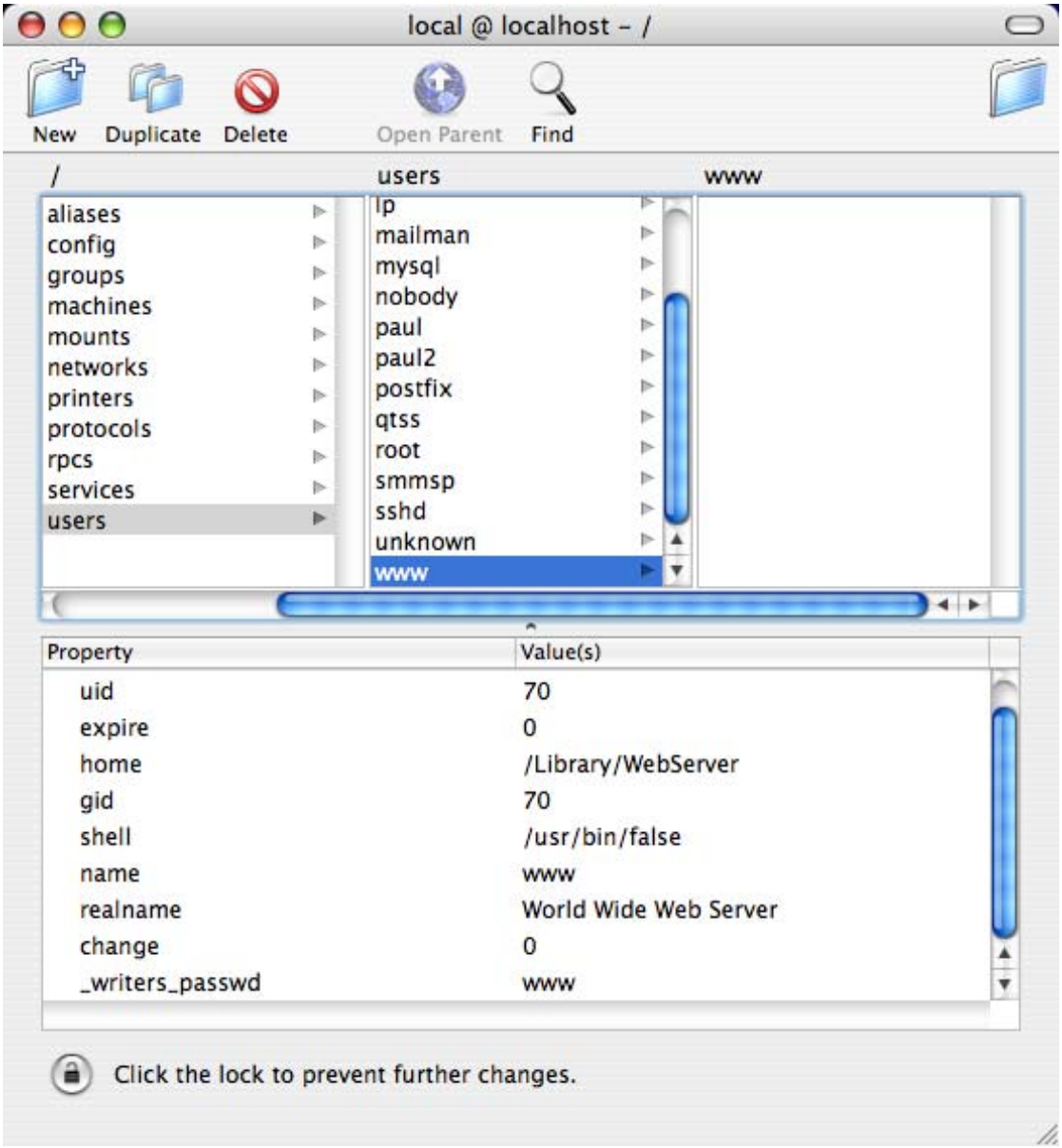


Εικόνα 33 - Παράθυρο Ρυθμίσεων Λογαριασμών Χρηστών

2.5.12. Ελέγχοντας τους λογαριασμούς χρηστών

Ένα ακόμα μέτρο προστασίας είναι και ο έλεγχος ότι κανείς άλλος λογαριασμός (όπου δεν φαίνεται στο παράθυρο Accounts) δεν έχει προστεθεί από την εγκατάσταση άλλων εφαρμογών και θα έχει ως συνέπεια τα υπολείμματα επισφαλών κωδικών. Αυτοί μπορεί να εκμεταλλευτούν από έναν κακόβουλο χρήστη για να λάβει τον έλεγχο του μηχανήματός σας.

- Applications -> Utilities -> NetInfo Manager -> Domain -> Open -> / -> OK -> / -> users
- Choose a system user -> Ensure it has no "passwd" entry
- If it does have a password entry, click the lock in the bottom left -> authenticate -> select the "passwd" line" -> Delete
- Close the window -> Save -> Update this copy



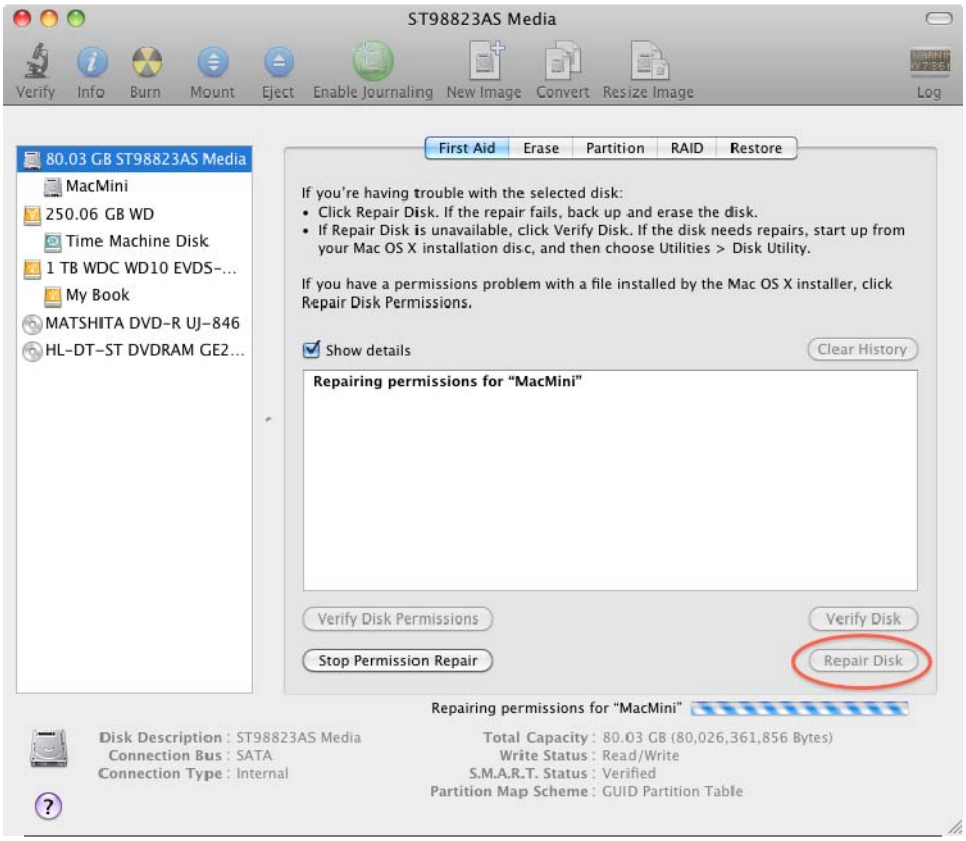
Εικόνα 34 – Παράθυρο Επεξεργασίας Χρηστών

2.5.13. Επισκευή αδειών πρόσβασης αρχείων (fix file permissions)

Με τον καιρό, οι ιδιότητες που αφορούν τις άδειες χρήσης και πρόσβασης των αρχείων μπορεί να αλλοιωθούν. Το φαινόμενο που δημιουργεί κάτι τέτοιο είναι οι εγκαταστάσεις εφαρμογών όπου δεν λαμβάνουν υπόψη τους τον σωστό καταμερισμό ασφάλειας των αρχείων.

Για να επιδιορθωθεί αυτό το φαινόμενο θα πρέπει ανά τακτά χρονικά διαστήματα θα εκτελέσετε την εφαρμογή Apple's Disk Utility προκειμένου να επαναφέρετε τις σωστές ιδιότητες αρχείων. Αυτό μπορείτε να το κάνετε με ως εξής :

- `Applications -> Utilities -> Disk Utility`
- `Select your / disk-partition`
- `First Aid -> Repair Disk Permissions`



Εικόνα 35 - Παράθυρο Διαχείρισης Σκληρών Δίσκων

Αυτό μπορεί να γίνει και από την γραμμή εντολών με δικαιώματα διαχειριστή

```
• /usr/sbin/diskutil repairPermissions /
```

Το αποτέλεσμα μπορεί να είναι ως εξής :

```
•
• Started verify/repair permissions on disk disk0s3 local
• Determining correct file permissions.
• We are using special permissions for the file or directory
• ./System/Library/Filesystems/cd9660.fs/cd9660.util. New permissions are
• 33261
• Permissions differ on ./private/var/log/install.log, should be -rw-r--r--
• , they are -rw-r-----
• Owner and group corrected on ./private/var/log/install.log
```

```
• Permissions corrected on ./private/var/log/install.log
• Permissions differ on ./private/var/log/wtmp, should be -rw-r--r-- , they
• are -rw-r-----
• Owner and group corrected on ./private/var/log/wtmp
• Permissions corrected on ./private/var/log/wtmp
• The privileges have been verified or repaired on the selected volume
• Verify/repair finished permissions on disk disk0s3 local
```

Μπορεί να επιλέξετε να προσθέσετε τα παραπάνω στα αρχεία cron του συστήματος ή του διαχειριστή, π.χ: /etc/weekly.local. Το diskutil είναι ανίκανο να επιδιορθώσει αυτόματα όλα τα προβλήματα που μπορεί να υπάρχουν στις άδειες πρόσβασης των αρχείων. Για να δείτε μια λίστα με τα πιθανά προβληματικά αρχεία, εκτελέσετε την ακόλουθη εντολή με δικαιώματα διαχειριστή :

```
• find / -type f \( -perm -4000 -o -perm -2000 \) \-exec ls -al {} \;
• 2>/dev/null
```

Για μία λίστα με όλα τα αρχεία που έχουμε δικαιώματα εγγραφής :

```
• find / -type f \( -perm -2 \) \-exec ls -al {} \; 2>/dev/null
```

Για μία λίστα με όλους τους φακέλους που έχουμε δικαιώματα εγγραφής :

```
• find / -type d \( -perm -2 \) \-exec ls -ald {} \; 2>/dev/null
```

Για μία λίστα με όλα τα ορφανά αρχεία :

```
• find / -nouser -o -nogroup \-exec ls -al {} \; 2>/dev/null
```

Βασιζόμενοι στα αποτελέσματα των παραπάνω εντολών , μπορεί να επιλέξετε να αλλάξετε ή να αφαιρέσετε τις άδειες πρόσβασης σε ορισμένα αρχεία χειροκίνητα. Βεβαιωθείτε ότι γνωρίζετε τον σκοπό του αρχείου που επιθυμείτε να αλλάξετε τα χαρακτηριστικά του. Απερίσκεπτες αλλαγές μπορεί να οδηγήσουν σε κατεστραμμένο σύστημα.

2.6. Ασφαλίζοντας το Swap File

Όταν ο υπολογιστής σας είναι σβηστός, τότε η μνήμη RAM, η μνήμη προσωρινής αποθήκευσης, δεν περιέχει δεδομένα. Τα λειτουργικά συστήματα χρησιμοποιούν την μέθοδο της εικονικής μνήμης RAM (swap file) για να αποφύγουν τυχών προβλήματα που οφείλονται σε περιορισμένη μνήμη RAM. Η μεταφορά δεδομένων μεταξύ φυσικής μνήμης (RAM) και εικονικής (Swap File) είναι συνεχής. Υπάρχει λοιπόν η πιθανότητα ευαίσθητα δεδομένα, πληροφορίες που πιστεύετε ότι έχουν σβηστεί, να παραμένουν στην εικονική μνήμη μέχρι εκείνη να αντικατασταθεί με νέα δεδομένα. Αυτές οι ευαίσθητες πληροφορίες μπορούν να προσπελαστούν από τρίτους, γιατί τα δεδομένα στην εικονική μνήμη δεν έχουν καμία κωδικοποίηση.

Όταν ο υπολογιστής σας περνάει σε κατάσταση αναμονής, γράφει τα περιεχόμενα της μνήμης RAM στο αρχείο /var/vm/sleepimage. Το αρχείο sleepimage περιέχει τα δεδομένα χωρίς κρυπτογράφηση.

Μπορείτε να αποτρέψετε τα ευαίσθητα δεδομένα της RAM να παραμείνουν δίχως κωδικοποίηση στον σκληρό δίσκο, αν ενεργοποιήσετε την επιλογή "secure virtual memory" στην καρτέλα General. Με αυτό τον τρόπο εφαρμόζεται κρυπτογράφηση στα περιεχόμενα του Swap File και του αρχείου /var/vm/sleepimage.

Για παράδειγμα, θα κάνουμε μια απλή προσπέλαση στο αρχείο swapfile, όπου μέσα σε αυτό αποθηκεύονται όλα τα δεδομένα της virtual memory. Ανοίγουμε το terminal και πληκτρολογούμε :

```
# cd /var/vm/
# strings -n 4 swapfile0 &gt; swapfile0-ascii
```

Τα αποτελέσματα είναι τα παρακάτω :

```
http://www.apple.com/SyncServices
Failed to login to account: %@
initWithCredentials: username is missing!
/SourceCache/DotMacSyncManager/DotMacSyncManage
r-308/src/SMSession.m
initWithCredentials: password is missing!
```

Βλέπουμε λοιπόν ότι στα περιεχόμενα του συγκεκριμένου αρχείου συμπεριλαμβάνονται σημαντικές πληροφορίες για την ασφάλεια του υπολογιστή μας, όπως κωδικοί και ιστορικό.

Αν ενεργοποιήσουμε την κωδικοποίηση, τότε όλες οι πληροφορίες του συστήματός μας που αποθηκεύονται στο swapfile ΔΕΝ είναι απλό κείμενο, οπότε είναι αδύνατο να προσπελαστούν.

2.6.1. Για να ενεργοποιήσετε το secure virtual memory

- Ανοίξτε την καρτέλα System Preferences.
- Επιλέξτε Security > General
- Επιλέξτε "Use secure virtual memory.
- Επανεκκίνηση.

Εικόνα 36 - Παράθυρο Γενικών Επιλογών Ασφάλειας

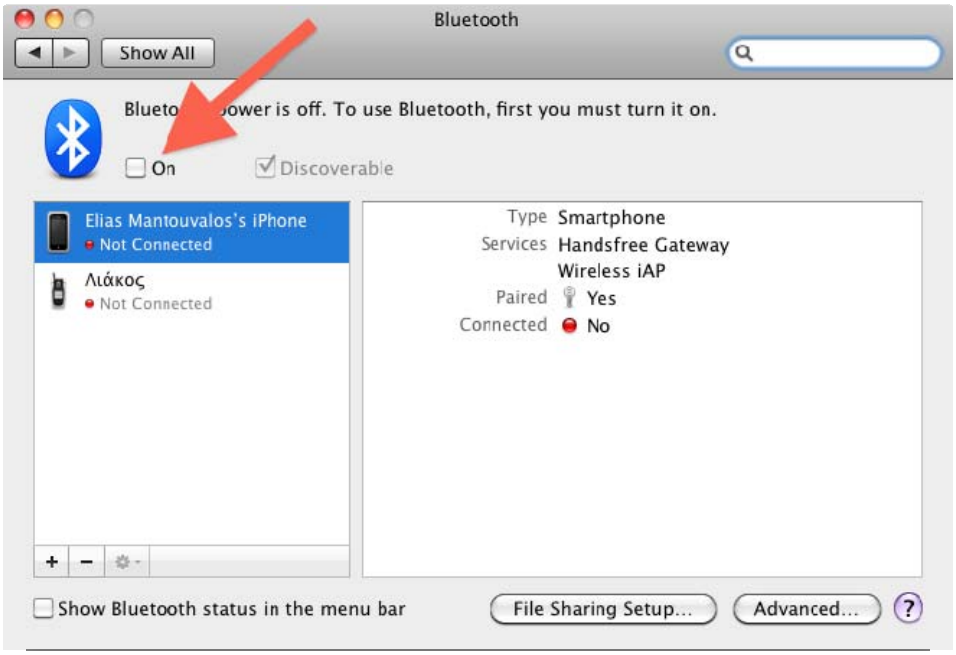
2.7. Ασφαλίζοντας το Bluetooth.

Το Bluetooth είναι μία ραδιοσυχνότητα (2.4 Ghz) μεταφοράς πληροφορίας που επιτρέπει να επικοινωνήσουν διάφορες μικροσυσκευές μεταξύ τους. Το πρωτόκολλο Bluetooth εγκαθιδρύει αυτό που ονομάζεται ως (PAN) Personal Area Network, επιτρέποντάς σας να έχετε το κινητό σας τηλέφωνο, το hands-free ακουστικό, το PDA και τον υπολογιστή να επικοινωνούν ασύρματα. Δυστυχώς, το Bluetooth έχει πολλά μειονεκτήματα στον τομέα της ασφάλειας. Στις παρακάτω ενότητες θα επικεντρωθούμε στις μεθόδους θωράκισης του πρωτοκόλλου στο Mac. Αυτές οι μέθοδοι μπορούν να εφαρμοστούν και σε άλλα, μη OS X μηχανήματα που λειτουργεί σε αυτά το bluetooth (π.χ. PDAs, κινητά τηλέφωνα κλπ).

2.7.1. Απενεργοποίηση του Bluetooth

Αν δεν χρησιμοποιείτε συχνά την σύνδεση Bluetooth του υπολογιστή σας, καλό θα ήταν να την απενεργοποιείτε :

- Apple menu -> System Preferences -> Bluetooth -> Settings
- "Turn Bluetooth Off"



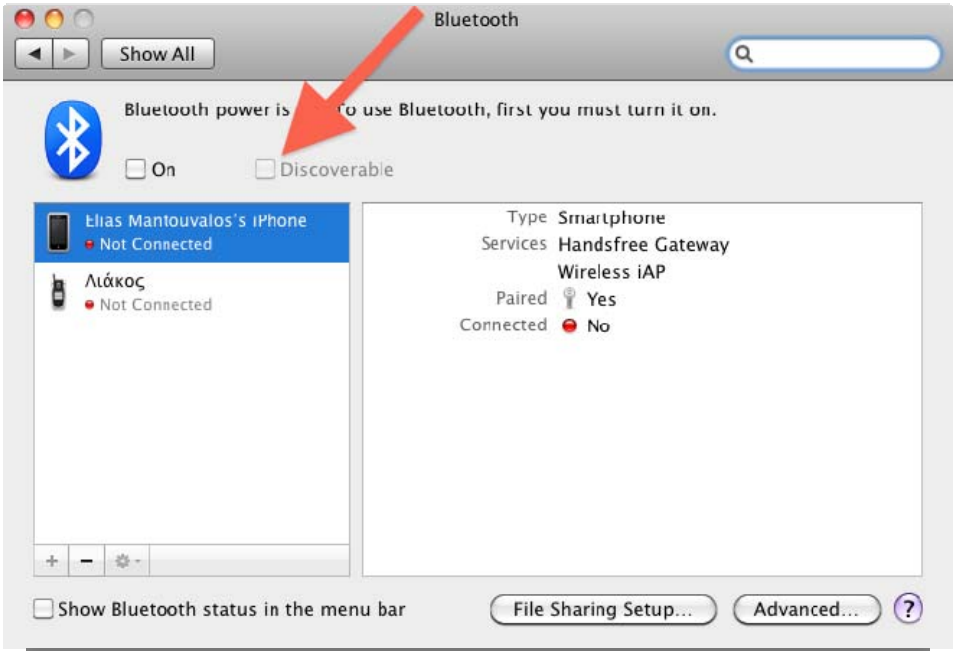
Εικόνα 37 - Παράθυρο Ρυθμίσεων Bluetooth

2.7.2. Ρυθμίστε την συσκευή να είναι αόρατη από ανιχνεύσεις

Οι συσκευές σας πρέπει να είναι ανιχνεύσιμες μόνο όταν ζευγαρώνουν με άλλες συσκευές Bluetooth. Μόλις ολοκληρωθεί αυτή η διαδικασία θα πρέπει να απενεργοποιείτε την ανιχνευσιμότητα της συσκευής σας. Αν έχει πραγματοποιηθεί το ζευγάρωμα, τότε οι συσκευές θα επικοινωνήσουν, ανεξάρτητα από το γεγονός ότι είναι ρυθμισμένες να είναι αόρατες.

Για να ρυθμίσετε το Mac σας να είναι αόρατο :

- Apple menu -> System Preferences -> Bluetooth -> Settings
- Uncheck "Discoverable"



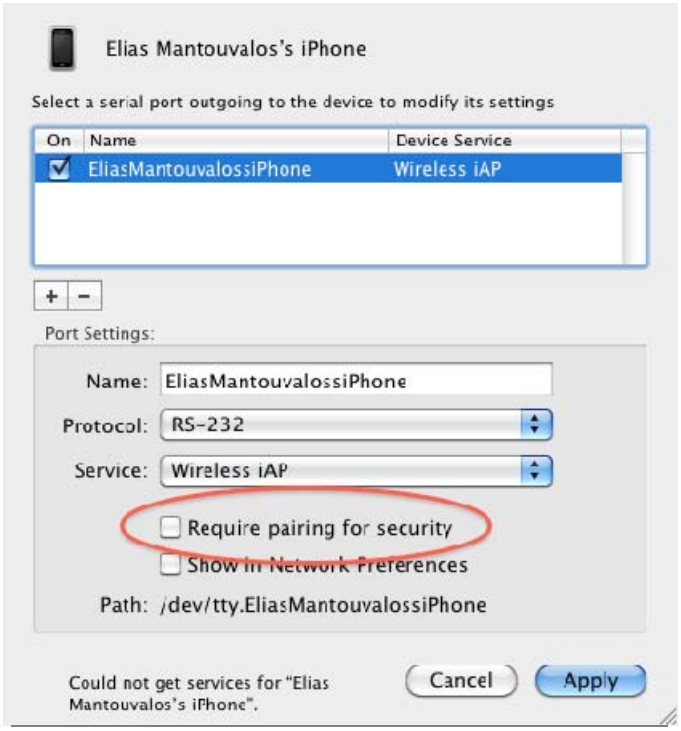
Εικόνα 38 - Παράθυρο Ρυθμίσεων Bluetooth

Να σημειωθεί ότι η ρύθμιση που καθιστά την συσκευή σας αόρατη, δεν την καθιστά τελείως μη ανιχνεύσιμη. Απλά την καθιστά δυσκολότερη να ανιχνευτεί.

2.7.3. Ενεργοποιήστε την αυθεντικοποίηση

Όταν ενεργοποιηθεί η αυθεντικοποίηση, οι συσκευές χρειάζονται έναν κωδικό για να ζευγαρώσουν μεταξύ τους. Για να ενεργοποιηθεί η αυθεντικοποίηση με κωδικό :

- `Apple menu -> System Preferences -> Bluetooth -> Settings`
- `Check "Require Pairing"`



Εικόνα 39 - Παράθυρο Ρυθμίσεων Bluetooth

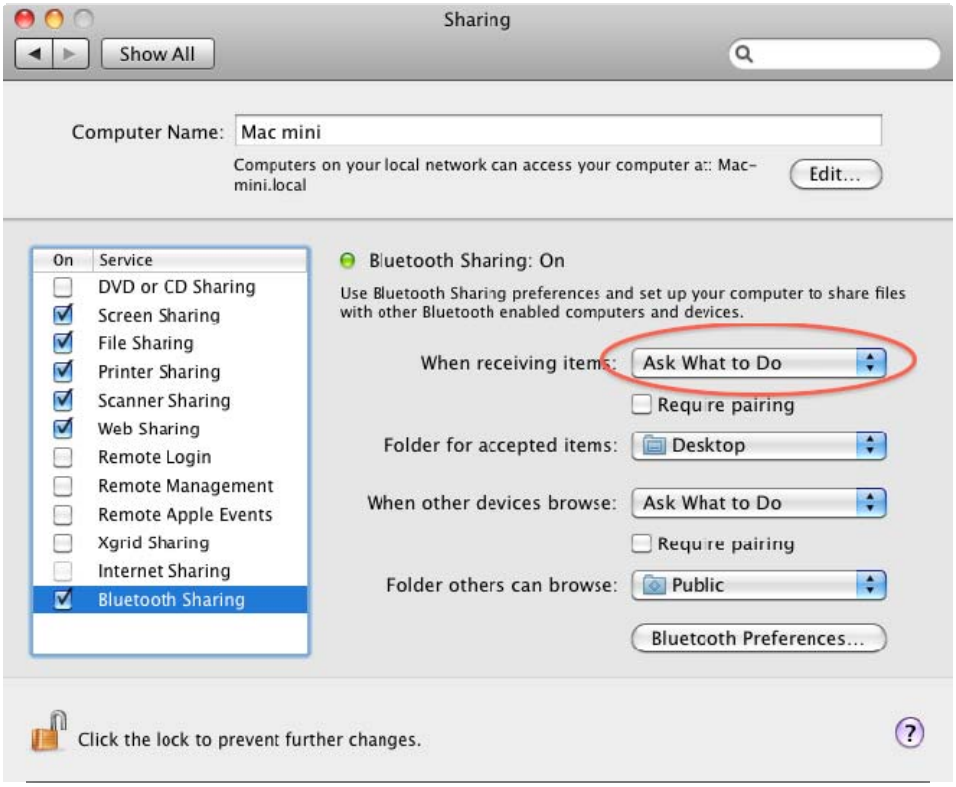
2.7.4. Ενεργοποιήστε την κωδικοποίηση

Αν ενεργοποιήσετε την κωδικοποίηση, το πλήθος των δεδομένων που μεταφέρονται μεταξύ των συσκευών, είναι κωδικοποιημένα με ένα κοινό κλειδί. Αυτό δυσκολεύει την υποκλοπή των δεδομένων, διότι δεν μπορούν να αναγνωστούν από τρίτους. Για να ενεργοποιήσετε την κωδικοποίηση του Bluetooth :

- Apple menu -> System Preferences -> Bluetooth -> Settings
- Check "Require Authentication" -> check "Use Encryption"

2.7.5. Απενεργοποίηση της αυτόματης αποδοχής αρχείων

Είναι προτιμότερο να απαιτείται ερώτηση όταν δεχόσαστε ένα αρχείο μέσω bluetooth. Με αυτό τον τρόπο περιορίζετε την πιθανότητα να δεχθείτε έναν επικίνδυνο ιό η Trojan στον υπολογιστή σας. Για να ενεργοποιήσετε την συγκεκριμένη δικλείδα ασφαλείας :



Εικόνα 40 - Παράθυρο Ρυθμίσεων Bluetooth

- Apple menu -> System Preferences -> Sharing -> Bluetooth Sharing
- Choose "When Receiving Items" -> "Ask What to Do"

3. Ασφάλεια Δικτύου

Η ακόλουθη ενότητα περιγράφει τις μεθόδους για ασφάλιση του Mac OS X από δικτυακές επιθέσεις.

3.1. Απενεργοποίηση υπηρεσιών (services)

Ως προεπιλογή το Mac OS X δεν έχει ενεργοποιημένες κάποιες υπηρεσίες δικτύου. Παρόλα αυτά, ορισμένες υπηρεσίες μπορεί να έχουν ενεργοποιηθεί δίχως την έγκρισή μας ή από κάποιο πρόγραμμα που εγκαταστήσαμε. Αυτή η ενότητα περιγράφει μεθόδους για την σίγουρη απενεργοποίηση άγνωστων υπηρεσιών.

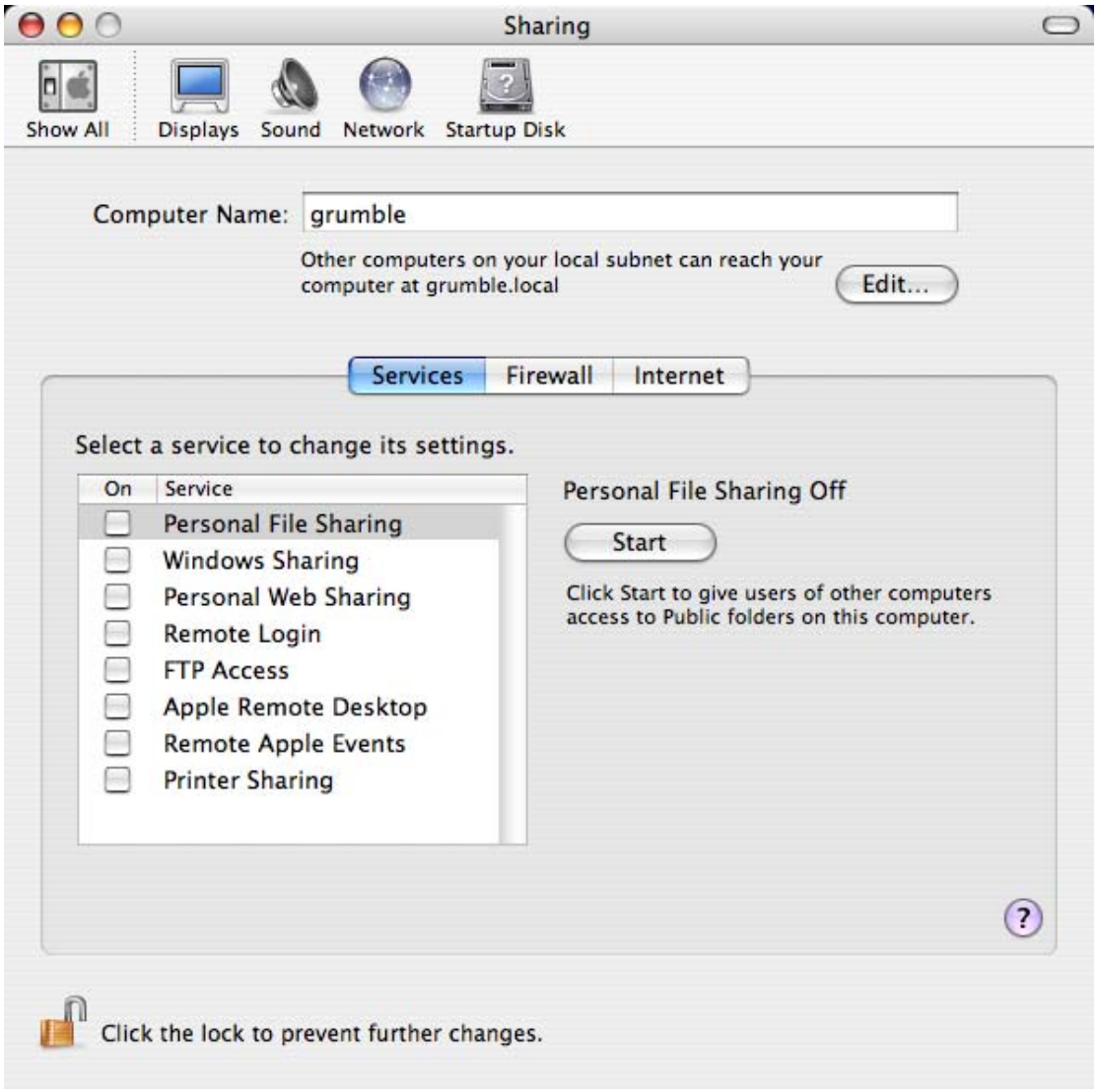
3.1.1. Sharing

Η καρτέλα Sharing της Apple είναι μία διεπαφή της υπηρεσίας xinetd και SystemStarter. Χρησιμοποιείται για να ενεργοποιηθούν ή να απενεργοποιηθούν ένα πλήθος από συχνές λειτουργίες του Internet όπως το SSH (“Remote Login”) και ο Apache web-server (“Personal Web Sharing”). Προεπιλεγμένα, το Mac OSX έρχεται με όλες τις λειτουργίες της καρτέλας Sharing ως απενεργοποιημένες , παρόλα αυτά, ορισμένοι χρήστες μπορεί να τις έχουν ενεργοποιήσει άθελά τους.

Για να απενεργοποιήσουμε όλες τις υπηρεσίες :

- `Apple menu -> System Preferences -> Sharing`

- Αποεπιλέγουμε οποιαδήποτε επιλεγμένη υπηρεσία



Εικόνα 41 – Παράθυρο Υπηρεσιών Κοινής Χρήσης

Βασικές πληροφορίες για το είδος της κάθε υπηρεσίας που επιλέγουμε να αλλάξουμε την κατάστασή της, υπάρχουν κάτω από το Start/Stop button.

Ο παρακάτω πίνακας είναι ενδεικτικός για τα ονόματα που έχει δώσει η Apple στις υπηρεσίες, τα κανονικά ονόματα που έχουν στο Internet και το λογισμικό που είναι υπεύθυνο για την λειτουργία τους.

Apple Service	Internet Service	Software
Personal File Sharing	AFP(overTCP)	AppleFileServer
Windows Sharing	SMB/CIFS	Samba
Personal Web Sharing	HTTP	Apache
Remote Login	SSH	OpenSSH
FTP access	FTP	tnftpd

Apple Remote Desktop	ARD	ARD Helper
Remote Apple Events	EPPC	AEServer
Printer Sharing	LPR/printer	CUPS

Πίνακας 4 – Πίνακας Υπηρεσιών Συστήματος

Αν θέλετε να έχετε απομακρυσμένη πρόσβαση στον Mac σας, το πρωτόκολλο SSH ("Remote Login"), θεωρείται ένα από τα ασφαλέστερα. Το SSH μπορεί επίσης να χρησιμοποιηθεί για μεταφορά αρχείων με την χρήση του SCP (Secure Copy) και του SFTP (Secure FTP). Μπορούμε επίσης να το χρησιμοποιήσουμε για δια μεταγωγή και άλλων υπηρεσιών, για παράδειγμα ARD ή VNC. link

Παρακάτω θα δείξουμε πως να περιορίζουμε ορισμένες Ips (είτε μέσω της υπηρεσίας xinetd ή ipfw) και να ασφαλίζουμε τις προεπιλεγμένες sshd ρυθμίσεις.

3.1.2. inetd

Το Mac OSX χρησιμοποιεί το xinetd Internet Super Server για να παρέχει ένα πλήθος από IP-based υπηρεσίες. Ορισμένες από αυτές ενεργοποιούνται και απενεργοποιούνται μέσω του παραθύρου ρυθμίσεων Sharing ενώ άλλες (συμπεριλαμβανομένων και εκείνου που αναφέρονται συχνά και ως "άχρηστες υπηρεσίες UNIX") δεν μπορούν να ρυθμιστούν από το ίδιο παράθυρο. Η πλήρης λίστα με τις εγκατεστημένες υπηρεσίες βρίσκεται στο /etc/xinetd.

Πίνακας 5 - Περιεχόμενα του αρχείου xinetd

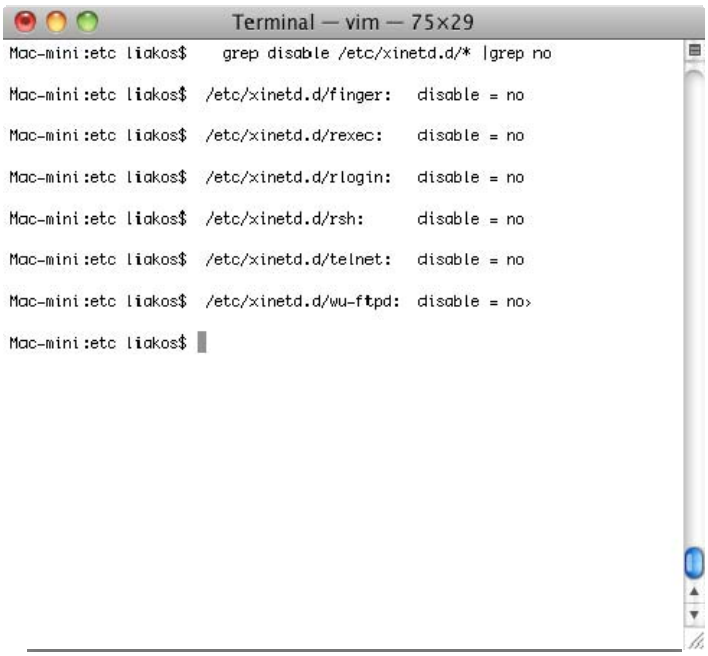
```
#
#  Sample  configuration  file  for
xinetd
#

defaults
{
    instances      = 25
    log_type                =   FILE
/var/log/servicelog
    log_on_success = HOST PID
    log_on_failure = HOST RECORD
#    only_from       = 128.138.193.0
128.138.204.0
#   only_from      = localhost
    disabled       = tftp
}

service imap
{
    socket_type    = stream
    protocol       = tcp
    wait           = no
    user           = root
    only_from          =  198.72.5.0
localhost
    banner                          =
/usr/local/etc/deny_banner
    server                          =
/usr/local/sbin/imapd
}
```

```
service telnet
{
    flags          = REUSE
    socket_type    = stream
    wait           = no
    user           = root
    server                          =
/usr/sbin/in.telnetd
    bind           = 192.168.1.11
    log_on_failure += USERID
}

#service chargen
#{
#    type           = INTERNAL
#    id             = chargen-stream
#    socket_type    = stream
#    protocol       = tcp
#    user           = root
#    wait           = no
#}

service xadmin
{
    type           = INTERNAL
    socket_type    = stream
    protocol       = tcp
    user           = root
    wait           = no
    port           = 7000
}
```

```
service telnet
{
    flags           = REUSE
    socket_type     = stream
    wait            = no
    user            = root
    redirect        = 192.168.1.1 23
    bind            = 127.0.0.1
    log_on_failure += USERID
}
```

Η λίστα οποιονδήποτε υπηρεσιών που έχουν ενεργοποιηθεί (είτε μέσω του Sharing preferences παραθύρου είτε με άλλον τρόπο), μπορεί να βρεθεί με την ακόλουθη εντολή :

```
• grep disable /etc/xinetd.d/* | grep no
```



Εικόνα 42 - Ενεργές υπηρεσίες στην Xinetd

Όποια υπηρεσία δεν απαιτείται από το σύστημα, καλό θα ήταν να απενεργοποιείται. Αυτό μπορεί να γίνει αν επεξεργαστούμε το αρχείο που εξάγεται με την παραπάνω εντολή και αν αλλάξουμε σε κάθε γραμμή την εντολή “disable = no” σε “disable = yes”. Για παράδειγμα, στην υπηρεσία SSH , το αρχείο μπορεί να εμφανίζεται ως εξής :

```
• service ssh
• {
• disable = yes
• socket_type = stream
```

```
• wait = no
• user = root
• server = /usr/libexec/sshd-keygen-wrapper
• server_args = -i
• groups = yes
• flags = REUSE IPv6
• session_create = yes
• }
```

Όταν γίνουν όλες οι απαραίτητες μετατροπές στο αρχείο, επανεκκινούμε την υπηρεσία xinetd με την εντολή :

```
• kill –HUP `cat /var/run/xinetd.pid`
```

Αν επιλέξουμε να έχουμε την υπηρεσία ενεργοποιημένη, μπορούμε να περιορίσουμε τις διευθύνσεις IP που εκείνη μπορεί να συνδεθεί, μέσω του xinetd ή μέσω του ενσωματωμένου firewall. Αν επιλέξουμε να κάνουμε την παραπάνω ενέργεια μέσω του xinetd, έχουμε την επιλογή “allow some, deny rest” ή την επιλογή “deny some, allow rest”.

Ως την τελευταία γραμμή (π.χ. Πριν το τελευταίο άγκιστρο) μέσα στο αρχείο ρυθμίσεων του xinetd, βάζουμε το εύρος των IP διευθύνσεων που θέλουμε να περιορίσουμε. Για να ακολουθήσουμε την τακτική “allow some, deny the rest”:

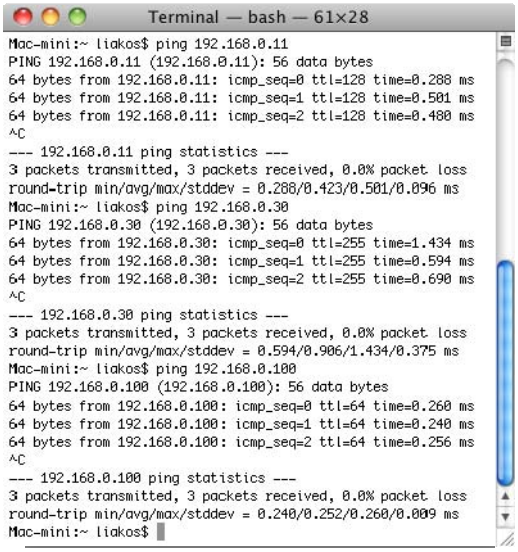
```
• only_from = <ip or subnet>, <ip or subnet>, <ip
  or subnet>
```

Ή τακτική “deny some, allow the rest”:

```
• no_access = <ip or subnet>, <ip or subnet>
```

Υπηρεσίες που είναι επίφοβες μπορούν να χειριστούν μέσω SSH με κρυπτογράφηση. Κάνοντας κάτι τέτοιο, θωρακίζουμε και αποκόπτουμε την υπηρεσία από τον έξω κόσμο και έχουμε πρόσβαση σε αυτή κάνοντας χρήση του πρωτοκόλλου SSH. Η εφαρμογή OpenSSH που είναι ενσωματωμένη στο Mac OSX έχει ενσωματωμένες λειτουργίες για να διευκολύνει την χρήση της σε συνεργασία με το xinetd και το εγκατεστημένο firewall.

Στο παρακάτω παράδειγμα έχουμε ένα τοπικό δίκτυο τριών υπολογιστών όπου μπορούμε να κάνουμε Ping σε όλους :

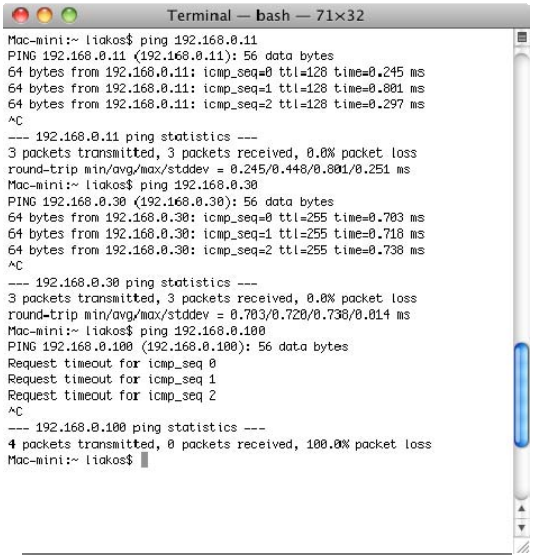


Εικόνα 43 – Ping σε τοπικό δίκτυο

Στη συνέχεια προσθέτουμε στο αρχείο xinetd του υπολογιστή μας την παρακάτω γραμμή :

```
• no_access = 192.168.0.100
```

Και επαναλαμβάνουμε το ping :

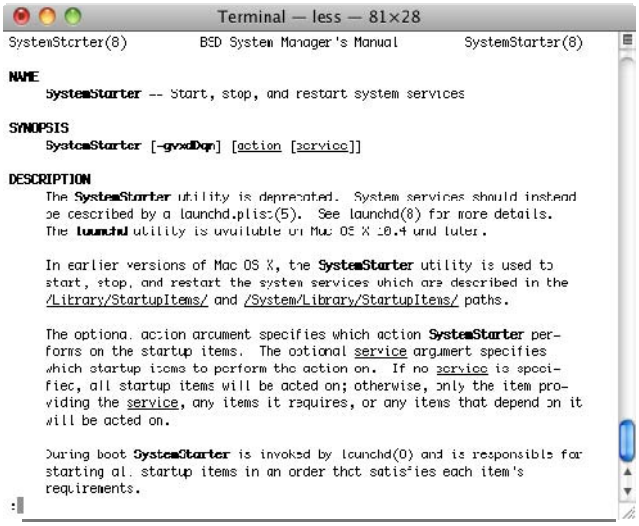


Εικόνα 44 – Ping σε τοπικό δίκτυο

Παρατηρούμε ότι ο υπολογιστής στο δίκτυο με IP 192.168.0.100 δεν είναι προσβάσιμος και αυτό οφείλεται στη ρύθμιση που κάναμε στο αρχείο xinetd.

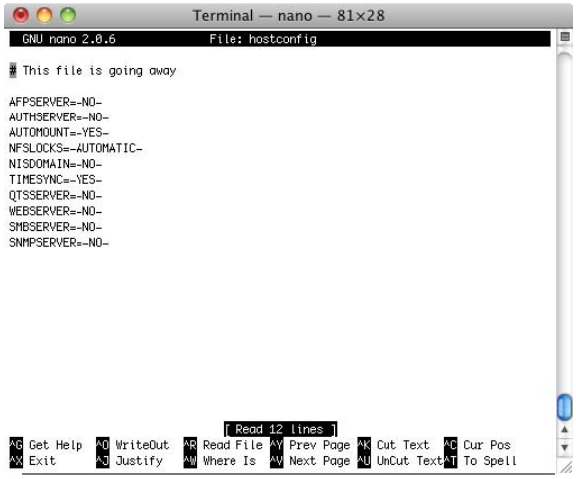
3.1.3. OSX hostconfig υπηρεσίες

Το Mac OS X χρησιμοποιεί κατά την εκκίνηση μία υπηρεσία που ονομάζεται SystemStarter, η οποία αντικαθιστά τα scrips εκκίνησης που χρησιμοποιούνται στα συστήματα UNIX. Συμπεριλαμβάνει χαρακτηριστικά που δεν βρίσκονται στα init scrips , όπως οι λίστες των αρχείων που απαιτούνται για μία υπηρεσία, παρά ο χειροκίνητος εντοπισμός αυτών μέσα από την χρήση του προγράμματος.



Εικόνα 45 - SystemStarter

Ορισμένα scrips της υπηρεσίας SystemStarter μπορούν να βρεθούν στο αρχείο /etc/hostconfig και μέσα από αυτά μπορούμε να επιλέγουμε την εκκίνησή τους κατά το ξεκίνημα του λειτουργικού ή όχι.



Εικόνα 46 - Hostcofig

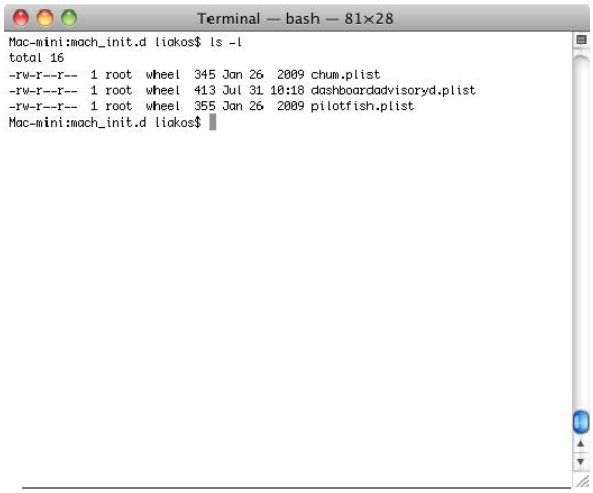
Ο ακόλουθος πίνακας αριθμεί τα αντικείμενα που μπορεί να βρεθούν στο αρχείο /etc/hostconfig μαζί με μία μικρή περιγραφή για την λειτουργία τους :

Υπηρεσία	Περιγραφή
AFPSERVER	Apple File Serving over TCP for "Personal File Sharing"
AUTHSERVER	Apple NetInfo Authentication service
AUTOMOUNT	Automatic mounting of NFS mount points (not to be confused with amd)
CUPS	Local printing services
IPFORWARDING	IP routing for other clients
IPV6	IP version 6 protocol support
MAILSERVER	The postfix SMTP mail server
NETINFOSERVER	Bind to a NetInfo server for directory and authentication access
NFSLOCKS	Network File System file locking support
NISDOMAIN	Bind to a NIS domain server for authentication
RPCSERVER	Remote Procedure Call support for numerous Unix services such as NFS
TIMESYNC	Run NTPd to maintain constant time synchronisation
QTSSERVER	Apple QuickTime Streaming Server modules
WEBSERVER	The Apache web server for "Personal Web Sharing"
SMBSERVER	Windows file sharing using Samba
DNSSERVER	BIND DNS server
COREDUMPS	Writes a core dump to disk in the case of a kernel panic
VPNSERVER	Apple's VPN service daemon (LT2P and PPTP)
CRASHREPORTER	Apple's crash logging service
XGRIDSERVER	Act as a server for Apple's grid computing software,xgrid
XGRIDAGENT	Act as a client for Apple's grid computing software,xgrid
ARDAGENT	Apple Remote Desktop server

Πίνακας 6 – Πίνακας Scrips

3.1.4. Άλλες υπηρεσίες του Mac OSX

Υπάρχουν και ορισμένα scripts του SystemStarter και του mach_init.d που δεν έχουν κάποια αναφορά στο αρχείο /etc/hostconfig προκειμένου να του επιτρέψουμε ή απαγορεύσουμε την λειτουργία τους. Τα συγκεκριμένα scrips απαιτούν ειδική εξέταση.



Εικόνα 47 – Scripts στο φάκελο mach_init.d

Το SystermStarter και mach_init αποθηκεύουν τα scrips σε τρεις τοποθεσίες :

- `/Library/StartupItems/`
- `/System/Library/StartupItems`
- `/etc/mach_init.d.`

Ένα παράδειγμα υπηρεσίας που ξεκινά από το StartupItems δίχως κάποια ρύθμιση στο /etc/hostconfig , είναι ο NFS server (nfsiod), που ξεκινά από την τοποθεσία /System/Library/StartupItems/NFS/NFS. Για να τον απενεργοποιήσουμε, θα πρέπει να αποκτήσουμε πρόσβαση ως root και να επεξεργαστούμε το scrip και να απενεργοποιήσουμε την γραμμή που ξεκινά με την εντολή nfsiod:

```
# nfsiod is the NFS asynchronous block I/O daemon, which implements
# NFS read-ahead and write-behind caching on NFS clients.
#nfsiod -n 4
```

Η υπηρεσία που είναι υπεύθυνη για την προσάρτηση εξωτερικών δίσκων και CD players, auto-mount daemon (ADM) μπορεί να απενεργοποιηθεί στο /System/Libraries/StartupItems/AMD/AMD. Ελέγχει επίσης το /etc/hostconfig για την εντολή "AMDSERVER:=-NO-" που πρέπει να προστεθεί χειροκίνητα (δεν περιλαμβάνεται στο /etc/hostconfig ως προεπιλογή).

Ένα προεγκατεστημένο σύστημα είναι αμφίβολο να έχει περαιτέρω αντικείμενα που δεν ελέγχονται από το /etc/hostconfig. Παρόλα αυτά , εφαρμογές που εγκαταστάθηκαν από τον χρήστη μπορεί να πρόσθεσαν αντικείμενα. Αν συμβαίνει κάτι τέτοιο, μπορούμε να το ελέγξουμε από τα περιεχόμενα του κάθε /System/Library/StartupItems/*/* και /etc/mac_init.d/* αρχείου για να διαπιστώσουμε ποιες υπηρεσίες ξεκινούν αυτόματα μαζί με το λειτουργικό

σύστημα. Αν όμως συμβαίνει κάτι τέτοιο, μπορούμε να εντοπίσουμε τις επιπλέον υπηρεσίες με την εντολή :

```
• /usr/sbin/lsof | grep LISTEN
```

3.2. Απενεργοποίηση των μεθόδων πρόσβασης φακέλων

Ως προεπιλογή, το OS X έχει ενεργοποιημένες ένα πλήθος υπηρεσιών που επιτρέπουν την πρόσβαση στους τοπικούς μας φακέλους και οι οποίες μπορούν να είναι ανοιχτές σε εξωτερικές επιθέσεις (π.χ. Η υπηρεσία LDAPv3 επιτρέπει την πρόσβαση ενός LDAP server από DHCP ως προεπιλογή, όπου κάτι τέτοιο μπορεί να υλοποιηθεί από έναν κακόβουλο DHCP server στο τοπικό δίκτυο).

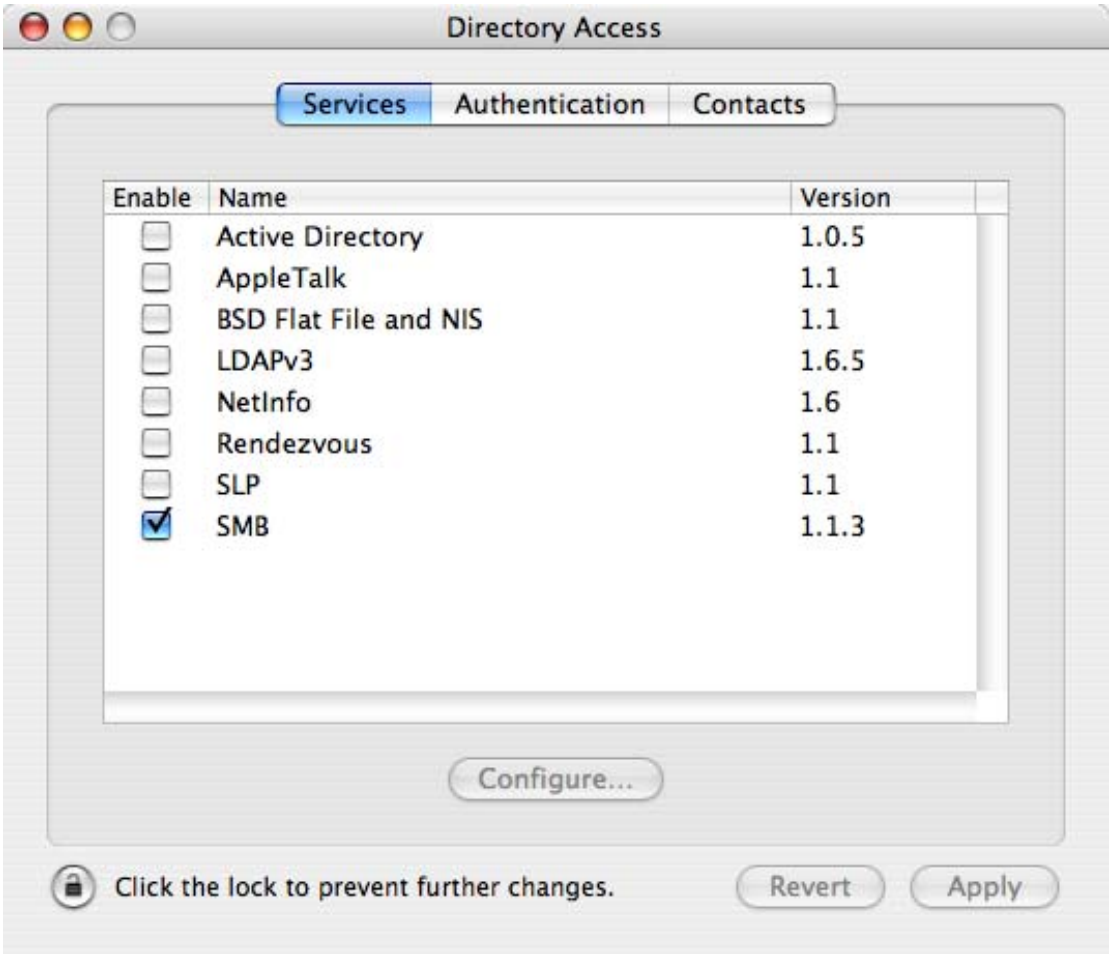
Για έναν μεμονωμένο υπολογιστή Mac , όπου αποτελεί απλώς έναν μεμονωμένο client, η πλειοψηφία (αν όχι το σύνολο) των υπηρεσιών δεν χρειάζεται. Ο ακόλουθος πίνακας περιγράφει την κάθε μέθοδο πρόσβασης φακέλων και την εκάστοτε περιγραφή τους :

Μέθοδος Πρόσβασης Δεδομένων	Περιγραφή
Active Directory	Windows 2000 domain file sharing and authentication
AppleTalk	Apples legacy protocol for discovering file and print services
BSD Flat File and NIS	/etc flat files and Unix Network Information Service (NIS) or Yellow Pages (yp) directory and authentication
LDAPv3	LDAP directory access and authentication
NetInfo	Apple’s directory access and authentication
Rendezvous	Apple multicast protocol for file, print, chat, music and other network services
SLP	Service Location Protocol – open standard file and print server discovery
SMB	Windows workgroup file and print sharing/serving

Πίνακας 7 – Πίνακας Υπηρεσιών Πρόσβασης

Για να επιλέξουμε τις μεθόδους που χρειαζόμαστε :

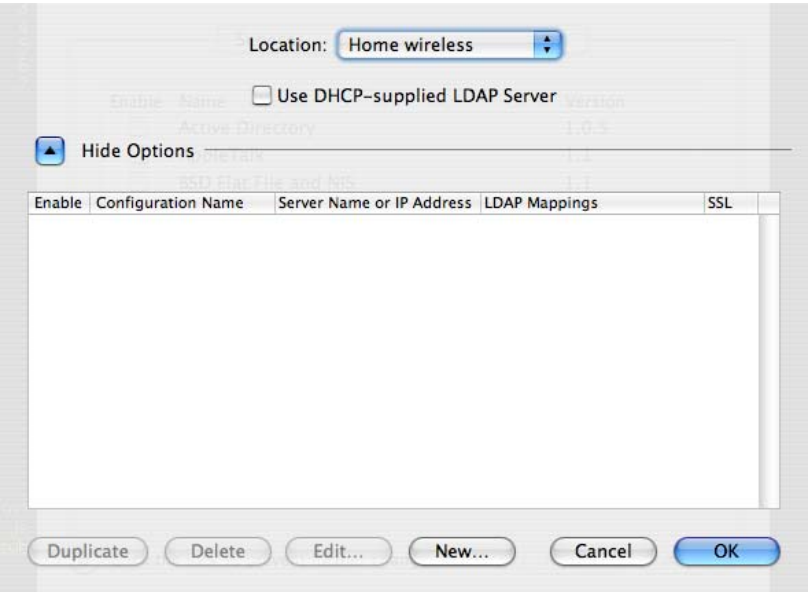
- `Applications -> Utilities -> Directory Access`
- `Uncheck unrequired services`



Εικόνα 48 – Παράθυρο Επιλογής Directory

Αν χρειάζεται να λειτουργήσει το LDAP για υπηρεσίες φακέλων (όπως ένα εταιρικό LDAP βιβλίο διευθύνσεων ηλεκτρονικού ταχυδρομείου), βεβαιωθήκατε ότι έχετε απενεργοποιήσει την παρεχόμενη DHCP LDAP Server επιλογή :

- `Applications -> Utilities -> Directory Access -> LDAPv3 -> Configure`
- `Uncheck "Use DHCP-supplied LDAP Server"`



Εικόνα 49 - Παράθυρο Επιλογής Δικτύου

3.3.Ασφάλεια με την χρήση VPN

Μπορείτε να προστατέψετε τα δεδομένα σας όταν τα στέλνετε διαμέσου μη ασφαλών δικτύων, όπως το Internet, με την χρήση μιας ασφαλής σύνδεσης δικτύου. Αυτό προλαμβάνει την μη εξουσιοδοτημένη πρόσβαση στα δεδομένα σας.

3.3.1. Ασφαλίζοντας την επικοινωνία απομακρυσμένης πρόσβασης

Μπορείτε να ασφαλίσετε την απομακρυσμένη πρόσβαση σε άλλα δύκτια με την χρήση του Εικονικού Ιδιωτικού Δικτύου (Virtual Private Network) - VPN. Ένα VPN αποτελείται από υπολογιστές ή δίκτυα (nodes) συνδεδεμένα με μία ιδιωτική ζεύξη (link) που μεταφέρει κωδικοποιημένα δεδομένα. Αυτή η ζεύξη εξομιώνει μία τοπική σύνδεση, σαν να έχουμε τον απομακρυσμένο υπολογιστή συνδεδεμένο στο τοπικό δίκτυο (LAN). Το VPN είναι μία παραλλαγή του IPSec πρωτοκόλλου, όπου με την σειρά του αυτό είναι μία ακόμα συλλογή πρωτοκόλλων που χρησιμοποιούνται για ασφάλεια του Internet Protocol (IP). Το IPSec κωδικοποιεί τα δεδομένα που μεταφέρονται από την IP.

3.3.2. VPN Security (L2TP και PPTP)

Υπάρχουν δύο πρωτόκολλα κωδικοποιημένης μεταφοράς δεδομένων : Το Layer Two Tunneling Protocol, Secure Internet Protocol (L2TP/IPSec) και το Point–to–Point tunneling Protocol (PPTP). Μπορείτε να ενεργοποιήσετε το καθένα ή και τα δύο από αυτά τα πρωτόκολλα. Το καθένα έχει τα πλεονεκτήματά του και τις απαιτήσεις του. Το L2TP over IPSec πρωτόκολλο παρέχει την μέγιστη δυνατή ασφάλεια επειδή λειτουργεί ήδη πάνω στο IPSec. Το PPTP δεν χρησιμοποιεί το IPSec πρωτόκολλο, γεγονός που το κάνει περισσότερο επισφαλές αν το χρησιμοποιήσουμε ως VPN πρωτόκολλο.

3.3.3. L2TP over IPSec

Το L2TP είναι μία προέκταση του PPTP (Point-to-point tunneling protocol) που χρησιμοποιείται από τους ISP για να ενεργοποιήσουν το VPN στο Internet. Το IPSec είναι ένα σύνολο από πρωτόκολλα ασφαλείας. Αν συνδυαστούν τα IPSec με το LT2P, το πρώτο κωδικοποιεί τα δεδομένα και το δεύτερο δημιουργεί την ασφαλή σύνδεση.

Ο συνδυασμός L2TP/IPSec κάνει χρήση ισχυρής IPSec κωδικοποίησης για να μεταφέρει τα δεδομένα μέσω τον ενδιάμεσων υπολογιστών. Βασίζεται στο Cisco L2F πρωτόκολλο.

Το IPSec απαιτεί πιστοποιητικά ασφαλείας για την μεταφορά ή προσδιορισμένους κωδικούς από τους ενδιάμεσους υπολογιστές που λαμβάνουν μέρος στην μεταφορά των δεδομένων. Οι συγκεκριμένοι κωδικοί δεν έχουν την κλασική έννοια του κλειδιού ή αποθηκευμένης φράσης, αλλά είναι περισσότερο αρχεία πρόσβασης που έχουν διαμοιραστεί ανάμεσα σε έμπιστους υπολογιστές.

Το L2TP είναι το προεπιλεγμένο πρωτόκολλο VPN που χρησιμοποιεί το OS X server γιατί έχει ισχυρή κωδικοποίηση δεδομένων και μπορεί να πιστοποιηθεί με την χρήση του Kerberos[29].

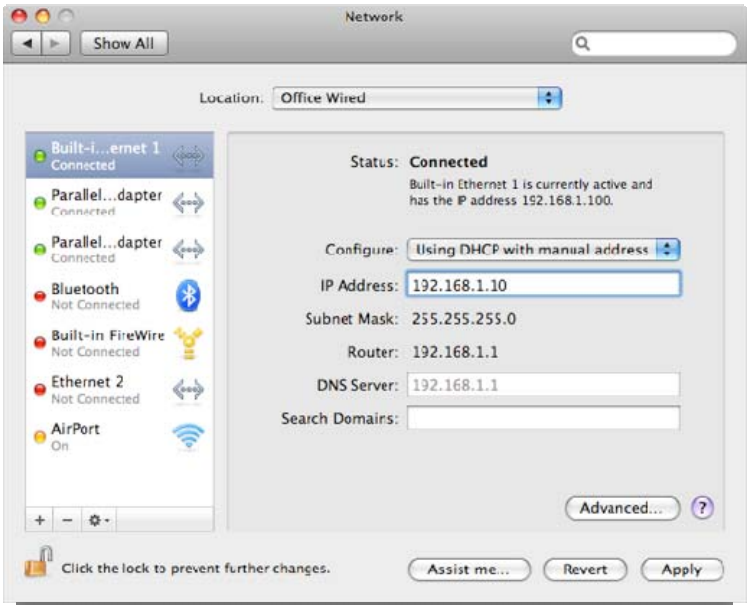
3.3.4. Ρύθμιση του IPSec

Οι υπολογιστές με OS X v10.5 είναι ρυθμισμένοι να κάνουν χρήση του DHCP για να αποκτούν μία διεύθυνση IP και πληροφορίες για έναν κατάλογο LDAP από τον εκάστοτε DHCP server. Όταν ο συγκεκριμένος server έχει τις απαραίτητες ρυθμίσεις LDAP, τότε εκείνες μεταφέρονται αυτόματα στους client υπολογιστές που έχουν εγκατεστημένο το OS X.

Οι ακόλουθες επιλογές ρυθμίζονται :

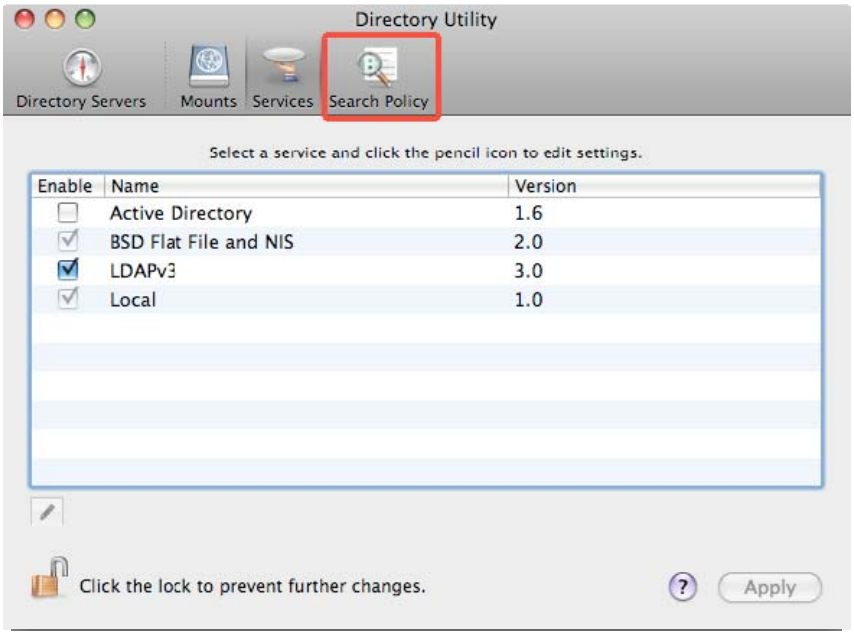
- Η προεπιλογή για το δίκτυο είναι το DHCP. Για να έχουμε πρόσβαση στις ρυθμίσεις του πρωτοκόλλου, επιλέγουμε System Preferences > Network preferences > Internal Ethernet Interface και από το pop up menu > “Using DHCP with manual address” ή “Using DHCP”

[29] http://web.mit.edu/kerberos/



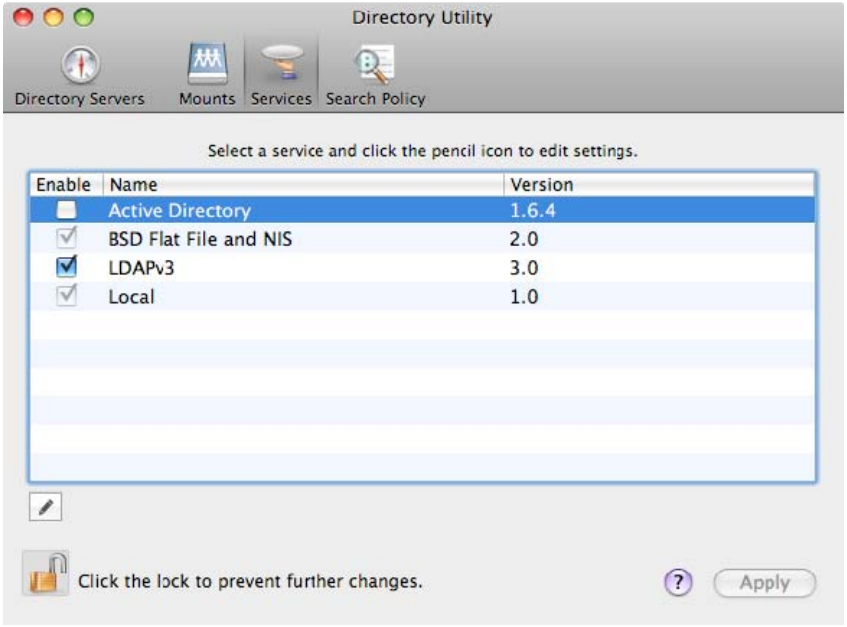
Εικόνα 50 - Παράθυρο Υπηρεσιών Δικτύου

- Σε περίπτωση που ο υπολογιστής σας ερευνηθεί στο τοπικό του δίκτυο, τότε γίνεται εμφανής από εκείνον που τον ψάχνει. Για αλλάξετε αυτή την ρύθμιση, επιλέξτε την εφαρμογή Directory Utility (στο /Applications/Utilities/) και επιλέξτε το Search Policy. Για μεταβολή των επιλογών, απαιτείται Administrator password.



Εικόνα 51 – Παράθυρο Υπηρεσιών Δικτύου

- Η χρήση πληροφοριών καταλόγου LDAP από τον εκάστοτε DHCP server είναι εξ΄ορισμού ενεργοποιημένη. Για να αλλάξετε συγκεκριμένη ρύθμιση επιλέγετε Directory Utility > Services > LDAPv3 και στην συνέχεια Configure.



Εικόνα 52 - Παράθυρο Ρυθμίσεων Δικτύου

3.3.5. Ρύθμιση του OS X client για την χρήση του VPN server

- Επιλέξτε System Preferences > Network.
- Επιλέξτε το plus button (+) στο κάτω μέρος των connection services και στην συνέχεια επιλέξτε το VPN από το pop-up menu.
- Από το menu επιλέξτε "L2TP over IPsec" ή "PPTP" ανάλογα με τις ανάγκες του δικτύου σας.
- Προσθέστε ένα όνομα στο Service Name field,και στη συνέχεια Create.
- Προσθέστε μία διεύθυνση DNS ή IP στο Server Address field π.χ. : gateway.example.com
- Προσθέστε το όνομα του λογαριασμού χρήστη στο πεδίο Account Name.
- Επιλέξτε Authentication Settings και προσθέστε τις πληροφορίες ρυθμίσεων User Authentication και Machine Authentication
- Πατήστε OK.

3.3.6. Ασφαλίζοντας το SSH

Το SSH (Secure Shell), παρέχεται στο OS X μέσω της πλατφόρμας ανοιχτού λογισμικού OpenSSH. Μπορεί να χρησιμοποιηθεί για ένα ένα ασφαλές αλληλεπιδραστικό κέλυφος εργασίας (SSH), ασφαλή μεταφορά αρχείων (SFTP), ασφαλή αντιγραφή αρχείων (scp), ασφαλές X-windows forwarding (X11Forwarding) και κρυπτογραφημένη διαμεταγωγή άλλων IP υπηρεσιών.

3.3.7. Γενικές παραμετροποιήσεις του SSHd

Το SSHd είναι εξαιρετικά παραμετροποιήσιμο και μπορεί να ασφαλιστεί ακόμα περισσότερο από τις προεπιλεγμένες του ρυθμίσεις. Το αρχείο ρυθμίσεων του server μπορεί να βρεθεί στην θέση /etc/sshd_config και προτείνουμε τις ακόλουθες αλλαγές σε σχέση με τις προεπιλεγμένες ρυθμίσεις :

```
• #Protocol 2,1
• (to)
• Protocol 2
• #PermitRootLogin yes
• (to)
• PermitRootLogin no
• Subsystem sftp /usr/libexec/sftp-server”
• (to)
• #Subsystem sftp /usr/libexec/sftp-server
```

3.3.8. Χρήση SSH κλειδιών για αυθεντικοποίηση

Θεωρείται ασφαλέστερο να αποκτούμε πρόσβαση σε ένα σύστημα με την ζεύξη κλειδιών SSH παρά με την χρήση κωδικών. Ένα σύστημα που μπορεί να ήταν υπό επίθεση, υπάρχει περίπτωση να έχει “μολυσμένες” τις εφαρμογές sshd ή αυθεντικοποίησης και να έχει αποστείλει τους προσωπικού σας κωδικούς στον επιτιθέμενο. Αν έχετε τους ίδιους κωδικούς για πολλά μηχανήματα (κάτι

εξαιρετικά επισφαλές), τότε ο κακόβουλος χρήστης μπορεί να έχει πρόσβαση σε όλα τα μηχανήματά σας.

Από την άλλη, αν αποκτάτε πρόσβαση με το ζεύγος κλειδιών του SSH , τότε αποτρέπετε τον κακόβουλο χρήστη από το να αποκτήσει πρόσβαση στα δεδομένα σας, ακόμα και αν χρησιμοποιείτε το ίδιο κλειδί SSH (με την ίδια πρόταση υπενθύμισης) για να αποκτήσετε πρόσβαση σε άλλα μηχανήματα. Για να απενεργοποιήσετε την αυθεντικοποίηση κωδικού :

- `#PasswordAuthentication yes -> PasswordAuthentication no`

Για να παράγουμε ένα ζεύγος κλειδιών SSH στο συνδεόμενο μηχάνημα (που υποτίθεται τρέχει το OpenSSH) :

- `user@host:~$ ssh-keygen -b 4096 -t dsa -C "Key for user@host Nov 2004"`
- `Generating public/private rsa key pair.`
- `Enter file in which to save the key (/Users/user/.ssh/id_rsa):`
- `Enter passphrase (empty for no passphrase):`
- `Enter same passphrase again:`
- `Your identification has been saved in /Users/user/.ssh/id_dsa.`
- `Your public key has been saved in /Users/user/.ssh/id_dsa.pub.`
- `The key fingerprint is:`
- `f3:99:d7:05:be:7f:41:42:64:97:b1:e7:d1:41:c9:08 Key for user@host Nov`
- `2004`

Η κωδικοποίηση DSA είναι αρκετά γρηγορότερη από την κωδικοποίηση RSA για την παραγωγή κλειδιών και ψηφιακών υπογραφών, αλλά υπάρχουν εκείνοι που υποστηρίζουν ότι το DSS έχει ορισμένα πιθανά κενά ασφαλείας στην διαδικασία υπογραφής σε μηχανήματα με περιορισμένη δυνατότητα τυχαίων αριθμών (διαδικασία εντροπίας).

Βεβαιωθείτε ότι συμπεριλάβατε και έναν κωδικό στο κλειδί σας, προκειμένου να το προστατέψετε στην περίπτωση που το απομακρυσμένο σύστημα καταληφθεί από κακόβουλους χρήστες.

Τοποθετήστε το /.ssh/id_dsa.pub από το απομακρυσμένο μηχάνημα στον φάκελο ~/.ssh/authorized_keys του Mac σας. Το κλειδί θα χρησιμοποιηθεί αυτόματα αντί για κωδικό στις υπηρεσίες SSH,SCP και SFTP απομακρυσμένης σύνδεσης.

3.3.9. Προώθηση του X11 μέσω του SSH

Στην περίπτωση που έχετε προγράμματα που χρησιμοποιούν το περιβάλλον X11 (UNIX) και θέλετε να εξαγάγετε τα δεδομένα τους πίσω σε απομακρυσμένα μηχανήματα, είναι προτιμότερο να χρησιμοποιήσετε την ενσωματωμένη δυνατότητα του SSH για X11 Forwarding. Αυτή βρίσκεται μέσα στο αρχείο ρυθμίσεων του /etc/sshd_config:

```
• #X11Forwarding no
• (to)
• X11Forwarding yes
```

Από το μηχάνημα που έχουμε φυσική πρόσβαση, ρυθμίζουμε την διαμεταγωγή SSH πληκτρολογώντας :

```
• ssh –X –l username <remote Mac>
```

3.3.10. Διαμεταγωγή άλλων υπηρεσιών IP μέσω SSH

Η υπηρεσία SSH μπορεί να χρησιμοποιηθεί για την διαμεταγωγή περισσοτέρων πρωτοκόλλων που υπό άλλες συνθήκες θα τα θεωρούσαμε ανασφαλή. Για παράδειγμα, μπορεί να επιθυμείτε να χρησιμοποιήσετε έναν VNC server (απομακρυσμένη πρόσβαση) που λειτουργεί σε ένα μηχάνημα OS X. Το πρωτόκολλο VNC από μόνο του δεν είναι κωδικοποιημένο και ο κωδικός του αποστέλλεται μέσω του δικτύου σε απλό κείμενο. Μία περισσότερο ασφαλής μέθοδος συνδεσιμότητας, είναι να εγκατασταθεί μία σύνδεση μέσω SSH , να κάνουμε διαμεταγωγή μίας VNC σύνδεσης στο μηχάνημα και να συνδεθούμε στη VNC θύρα μέσω της SSH σύνδεσης.

Για παράδειγμα, προκειμένου να εγκαταστήσουμε σε έναν απομακρυσμένο Mac μια σύνδεση TCP στην θύρα 5900 (προεπιλογή για το VNC), θα πρέπει να εκτελέσουμε την εντολή :

```
• ssh –N –L 5900:127.0.0.1:5900 <remote Mac>
```

Η παραπάνω εντολή συνδέει το SSH με την θύρα 5900 στο τοπικό μηχάνημα και την προωθεί , μέσω SSH , στην θύρα 5900 του απομακρυσμένου Mac. Τώρα θα θέσουμε τον VNC client στην διεύθυνση 127.0.0.1 (το loopback του τοπικού μηχανήματος) στην θύρα 5900 και θα συνδεθούμε με κωδικοποίηση στον απομακρυσμένο Mac.

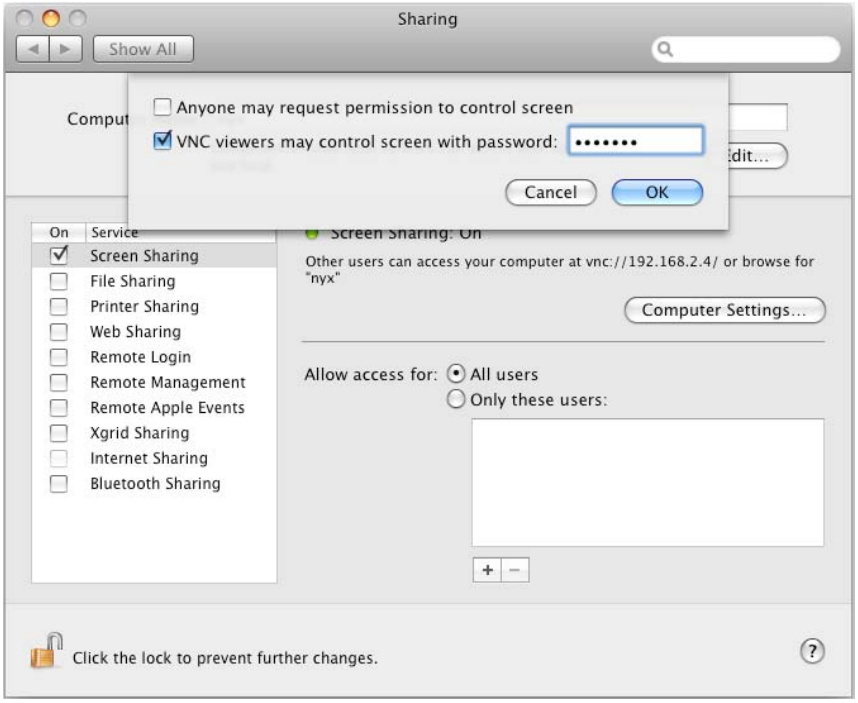
3.3.11. Επανεκκίνηση της υπηρεσίας sshd ύστερα από αλλαγή του αρχείου ρυθμίσεων

Επειδή το Mac OS X “τραβάει” την υπηρεσία sshd από τον server xinetd αντί να το χρησιμοποιεί σαν μεμονωμένο server, δεν υπάρχει η ανάγκη για επανεκκίνηση

ύστερα από αλλαγή στο αρχείο ρυθμίσεων sshd_config. Οι αλλαγές εφαρμόζονται στην αμέσως επόμενη σύνδεση στην υπηρεσία.

3.4.Screen Sharing (VNC)

Η υπηρεσία screen sharing βασίζεται στο πρωτόκολλο VNC. Μπορείτε να ρυθμίσετε τον υπολογιστή σας ώστε να παρέχετε απομακρυσμένο διαμοιρασμό οθόνης σε τρίτους. Αν η συγκεκριμένη υπηρεσία είναι ενεργοποιημένη, τότε απομακρυσμένοι χρήστες έχουν την δυνατότητα να βλέπουν ότι βλέπετε και εσείς στην οθόνη του υπολογιστή σας, να έχουν την δυνατότητα να επεξεργαστούν τα δεδομένα σας, ακόμα και να σβήσουν τον υπολογιστή.



Εικόνα 53 – Παράθυρο Ρυθμίσεων Απομακρυσμένης Διαχείρησης

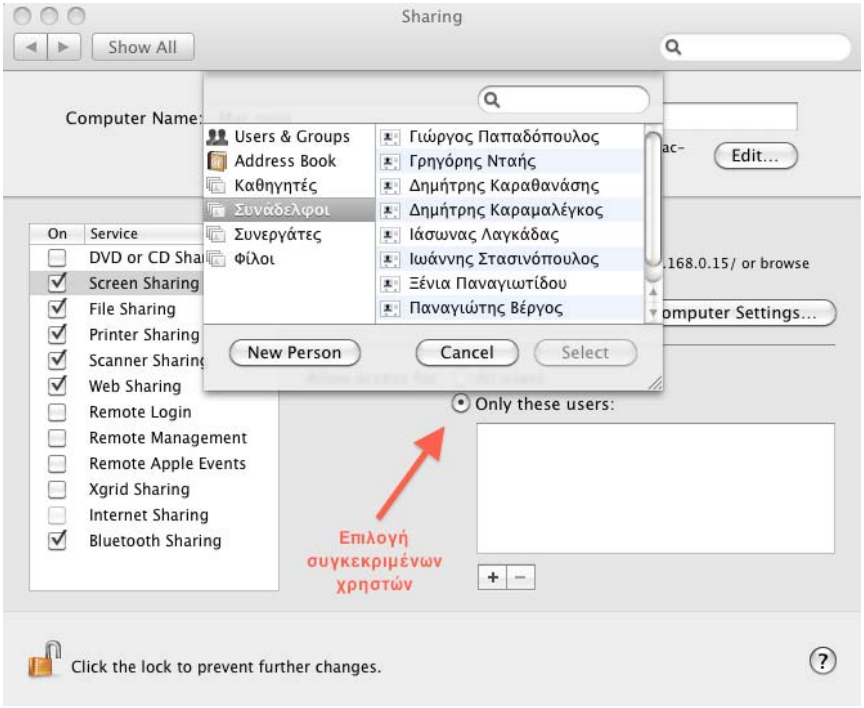
Το VNC επιτρέπει σε οποιονδήποτε με τα κατάλληλα πιστοποιητικά (user name - password) να αποκτήσει έλεγχο στον υπολογιστή σας. Τα δεδομένα που μεταφέρονται διαμέσου των υπολογιστών δεν είναι κωδικοποιημένα, οπότε καλό είναι η χρήση της υπηρεσίας να γίνεται σε κλειστό και ασφαλές δίκτυο με δίχως πρόσβαση στο Internet. Ως προεπιλογή, ο διαμοιρασμός οθόνης δεν είναι ενεργοποιημένος στο OS X και καλό θα ήταν να παραμένει απενεργοποιημένος αν δεν υπάρχει λόγος χρήσης του.

Αν επιλέξετε να έχετε ενεργοποιημένη την υπηρεσία στον δικό σας υπολογιστή, δηλαδή να ενεργείτε ως server, τότε θα πρέπει να ορίσετε έναν κωδικό. Επίσης, μία καλή πρακτική είναι να περιορίσετε την πρόσβαση σε συγκεκριμένες διευθύνσεις IP.

Αν επιθυμείτε ακόμα περισσότερη ασφάλεια, μπορείτε να επιλέξετε την αποδοχή συνδέσεων μόνο μέσα από το τοπικό δίκτυο με την χρήση ssh διαμεταγώγησης. Με αυτό τον τρόπο τα δεδομένα μεταξύ client και server θα είναι κωδικοποιημένα.

3.4.1. Λίστες Πρόσβασης

Στην ρύθμιση για απομακρυσμένη πρόσβαση, μια πολύ καλή πρακτική είναι να εξουσιοδοτείτε συγκεκριμένους χρήστες να αναλαμβάνουν τον έλεγχο του υπολογιστή σας. Η προεπιλεγμένη ρύθμιση πρέπει να αλλάξει από το "All users" στο "Only these users". Στην περίπτωση που δημιουργήσετε έναν χρήστη για απομακρυσμένη πρόσβαση, καλό θα ήταν να τοποθετήσετε έναν ισχυρό κωδικό με την χρήση του Password Assistant.

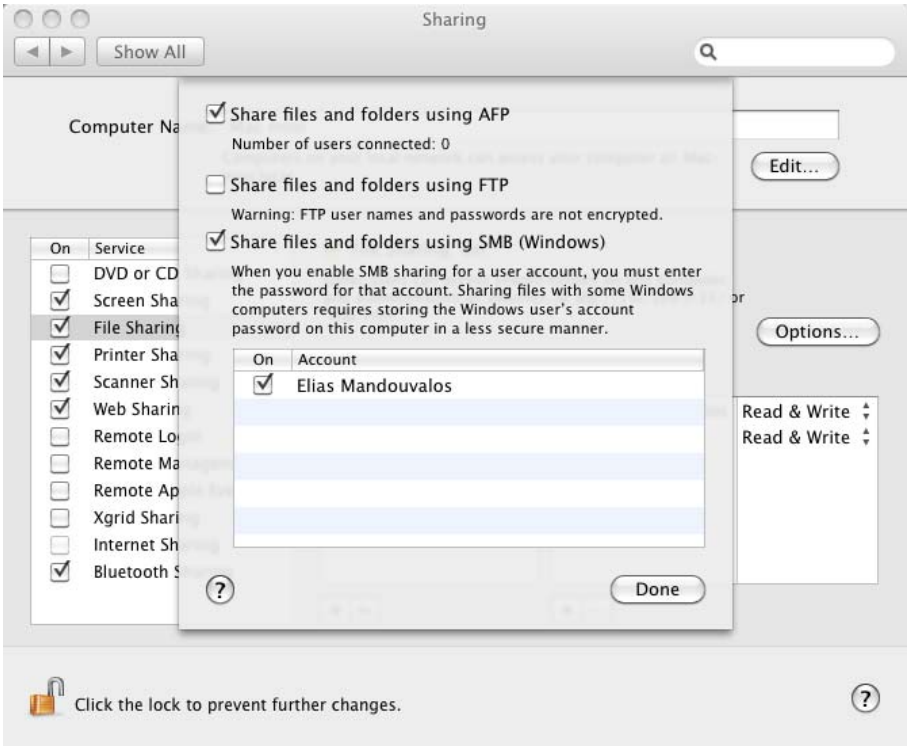


Εικόνα 54 – Επιλογή χρηστών VLC

Μπορείτε να ενεργοποιήσετε και την χρήση κωδικού για την υπηρεσία απομακρυσμένου ελέγχου. Αυτό θα σας επιτρέψει να γίνεται χρήση προγραμμάτων πρόσβασης και από τρίτους κατασκευαστές που απαιτούν την χρήση κωδικού. Ο κωδικός της υπηρεσίας διαφέρει από τον κωδικό του απομακρυσμένου χρήστη, αλλά απαιτούνται και οι δυο προκειμένου να αποκτήσει κάποιος πρόσβαση στον υπολογιστή σας.

3.4.2. Διαμοιρασμός αρχείων (AFP, FTP και SMB)

Μπορείτε να ρυθμίσετε τον υπολογιστή σας ώστε να έχει την δυνατότητα να διαμοιράζεται τα αρχεία του, κάνοντας χρήση των πρωτοκόλλων Apple Filing Protocol (AFP), File Transfer Protocol (FTP), ή Server Message Block (SMB). Ακόλουθα μπορούν να ρυθμιστούν και οι άδειες πρόσβασης για ανάγνωση, εγγραφή ή τροποποίηση συγκεκριμένων αρχείων ή φακέλων στον υπολογιστή σας.



Εικόνα 55 – Επιλογή πρωτοκόλλου διαμερισμού αρχείων

3.4.3. Διαμοιρασμός αρχείων

Όταν μοιράζεστε αρχεία και φακέλους στον υπολογιστή σας, τότε επιτρέπετε σε χρήστες να έχουν πρόσβαση στα δεδομένα του υπολογιστή σας. Αν επιτρέψετε κάτι τέτοιο, θα πρέπει να έχετε γνώση ποιος έχει πρόσβαση στα αρχεία σας, τις εκάστοτε άδειες πρόσβασης και το είδος του πρωτοκόλλου που χρησιμοποιήθηκε για την πρόσβαση των αρχείων και φακέλων. Για να υπάρξει ασφάλεια στον διαμοιρασμό αρχείων, θα πρέπει να έχουν ρυθμιστεί οι άδειες πρόσβασης για τους χρήστες. Αν δεν έχει γίνει κάτι τέτοιο, τότε υπάρχει ένα μεγάλο κενό ασφάλειας στην πρόσβαση του υπολογιστή σας.

Ανάλογα με τις απαιτήσεις σας, μπορείτε να μοιραστείτε αρχεία με την χρήση των πρωτοκόλλων AFP, FTP, ή SMB. Όταν μοιράζεστε αρχεία με το πρωτόκολλο AFP, τα προσωπικά στοιχεία των χρηστών κωδικοποιούνται όταν αυτοί αποκτούν πρόσβαση στον υπολογιστή σας για να προσπελάσουν τα αρχεία σας. Με την χρήση του πρωτοκόλλου SMB, οι κωδικοί και τα ονόματα χρηστών επίσης κωδικοποιούνται όταν πραγματοποιείται πρόσβαση. Παρόλα αυτά, οι κωδικοί του

SMB δεν αποθηκεύονται με ασφάλεια στον υπολογιστή σας.

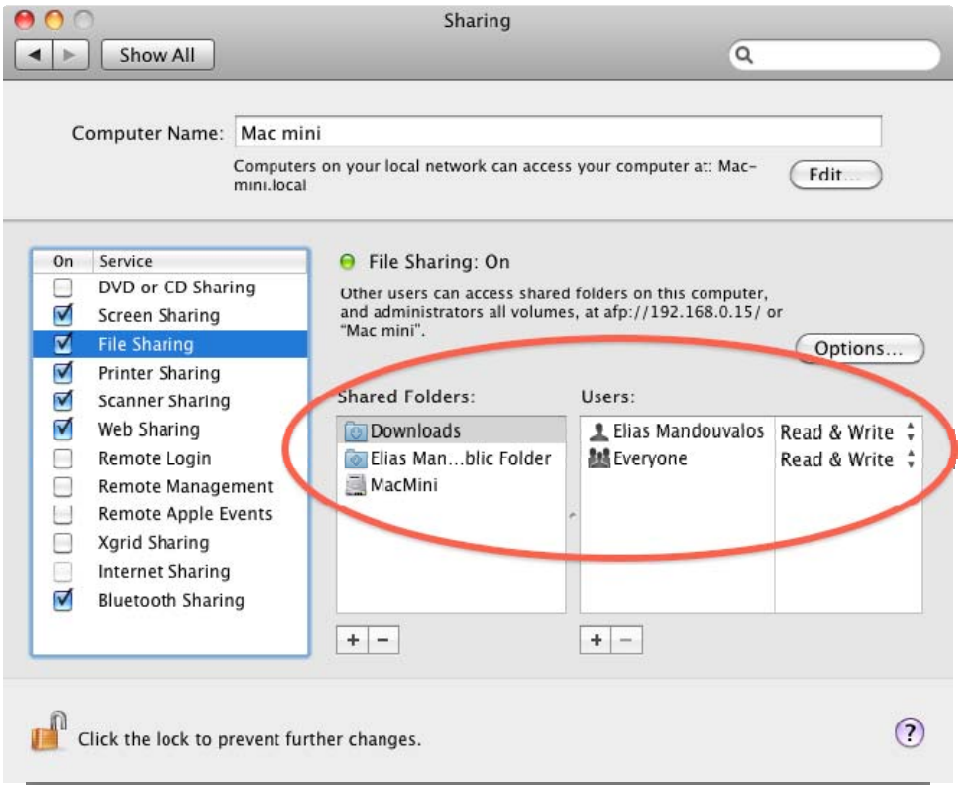
Το FTP πρωτόκολλο δεν πραγματοποιεί καμία κωδικοποίηση προσωπικών δεδομένων. Αυτό διευκολύνει τους κακόβουλους χρήστες να αποκτήσουν τους κωδικούς και ονόματα χρηστών και συνεπώς να έχουν πρόσβαση στα δεδομένα σας. Το FTP είναι ένα ξεπερασμένο πρωτόκολλο επικοινωνίας και καλό θα ήταν να το αποφεύγετε. Αν χρειαστεί να γίνει χρήση του, τότε καλό θα ήταν τα δεδομένα που μεταφέρονται να είναι κωδικοποιημένα.

Εικόνα 56 - Επιλογή πρωτοκόλλου sharing

Ο διαμοιρασμός αρχείων είναι ένα χαρακτηριστικό των σύγχρονων λειτουργικών συστημάτων. Είναι εξαιρετικά χρήσιμη αυτή η δυνατότητα σε περιβάλλον που απαιτείται συχνή μεταφορά αρχείων από υπολογιστή σε υπολογιστή. Αν δεν θέλετε πρόσβαση στα αρχεία του υπολογιστή σας, ένας εναλλακτικός υπολογιστής που θα έχει τον ρόλο του file server θα μπορεί να περιορίσει την πρόσβαση στον δικό σας. Ο διαμοιρασμός των αρχείων είναι στο OS X απενεργοποιημένος και καλό θα ήταν να παραμείνει έτσι αν δεν χρειάζεται η χρήση του. Με αυτό τον τρόπο μπορείτε να αποτρέψετε τυχόν μη εξουσιοδοτημένη πρόσβαση.

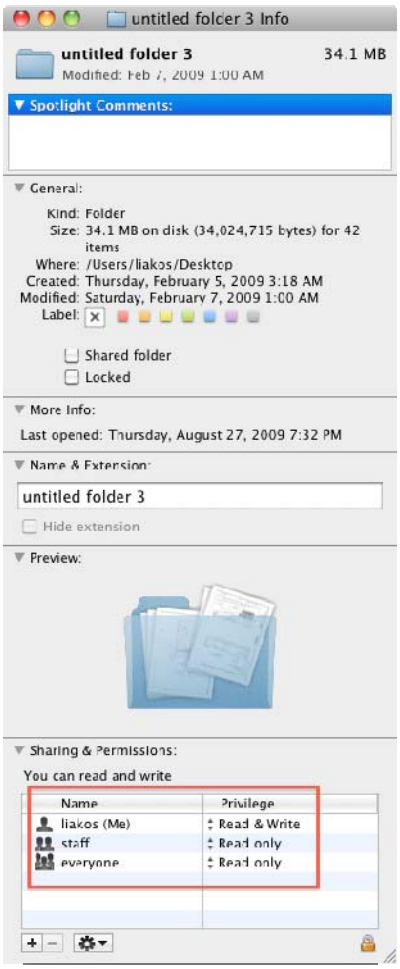
3.4.4. Περιορισμός πρόσβασης

Όταν ρυθμίζετε τον διαμοιρασμό αρχείων στον υπολογιστή σας, μπορείτε να θέσετε περιορισμούς πρόσβασης σε επιλεγμένους χρήστες. Μπορείτε να επεκτείνετε τους περιορισμούς σε συγκεκριμένα αρχεία ή φακέλους.



Εικόνα 57 - Περιορισμοί πρόσβασης

Η προεπιλογή για τον διαμοιρασμό αρχείων θα πρέπει να αλλάξει από την επιλογή "All users" στο "Only these users". Η επιλογή "All users" περιλαμβάνει όλους τους τοπικούς χρήστες του υπολογιστή και όλους τους χρήστες στο τοπικό σας δίκτυο.

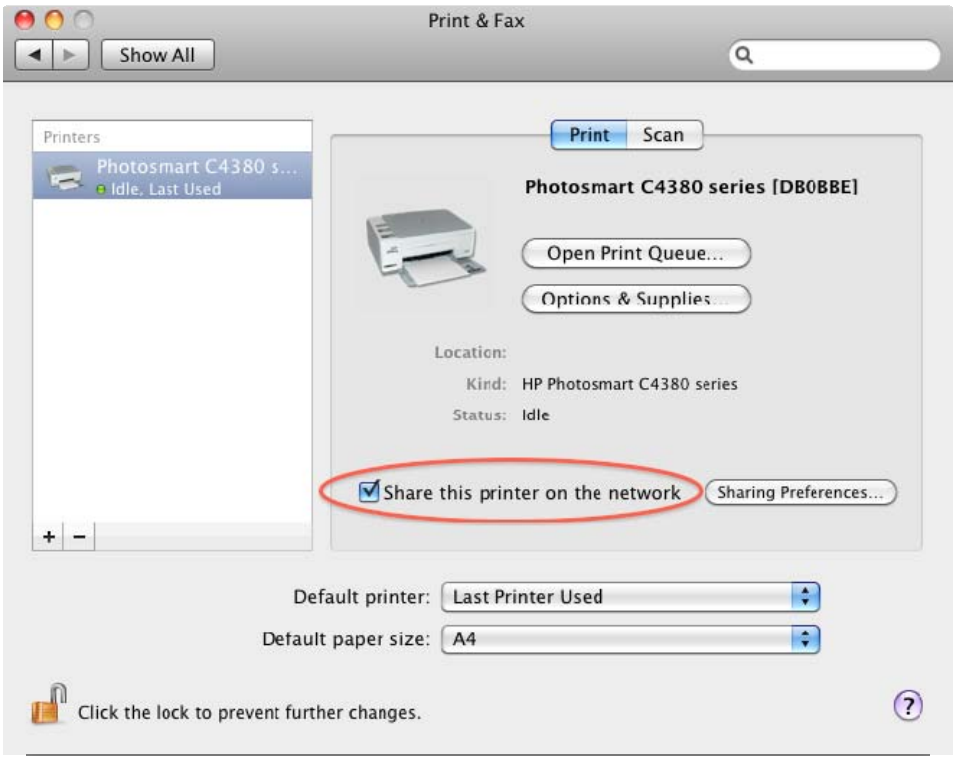


Εικόνα 58 - Παράθυρο ιδιοτήτων φακέλου

Αν μοιράζεστε αρχεία με χρήστες των Windows θα πρέπει να κάνετε χρήση του πρωτοκόλλου SMB. Θα πρέπει να δημιουργήσετε ισχυρούς κωδικούς για τους χρήστες που θα έχουν πρόσβαση στον υπολογιστή σας, γι'αυτό θα ήταν καλό να κάνετε χρήση του εργαλείου Password Assistant. Οι κωδικοί που δημιουργείτε, δεν αποθηκεύονται encrypted στον υπολογιστή σας.

3.4.5. Printer Sharing (CUPS)

Ο Διαμοιρασμός Εκτυπωτών επιτρέπει στους χρήστες άλλων υπολογιστών να έχουν πρόσβαση στον εκτυπωτή που έχετε εγκατεστημένο στον υπολογιστή σας. Καλό θα ήταν να έχετε έναν υπολογιστή που θα έχει τον ρόλο του printer server. Με αυτό τον τρόπο αποφεύγετε την κίνηση δεδομένων εκτύπωσης από τον υπολογιστή σας.



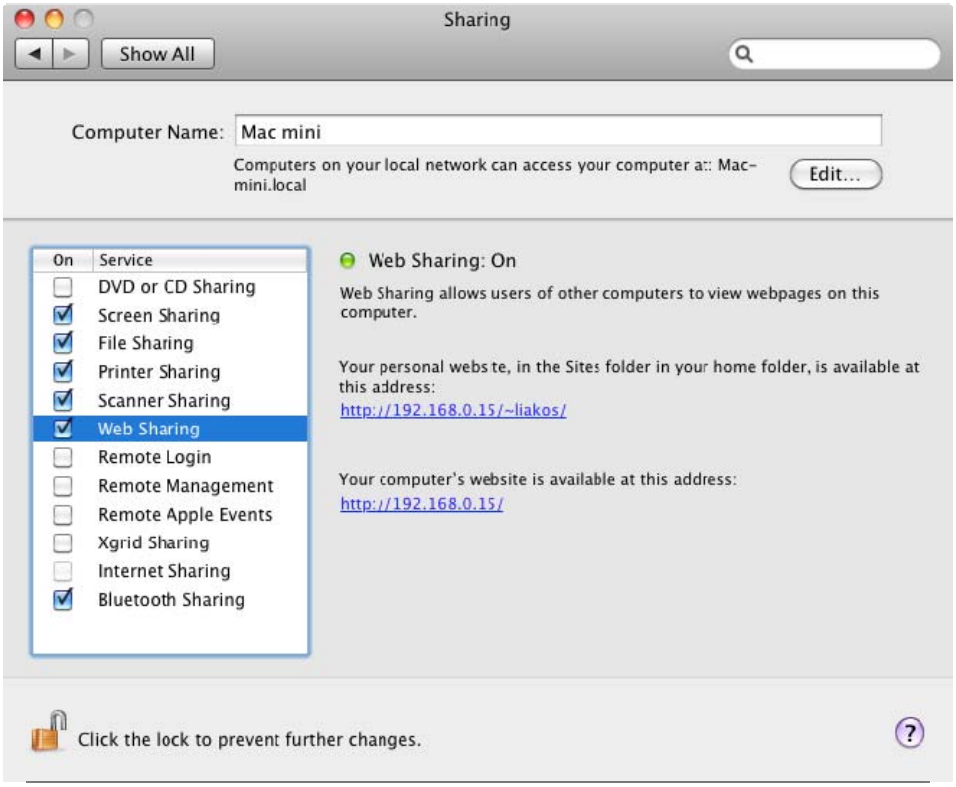
Εικόνα 59 - Ιδιότητες εκτυπωτή

3.4.6. Web Sharing (HTTP)

Μπορείτε να χρησιμοποιήσετε τον Apache web server, όπου περιλαμβάνεται στο Mac OS X, για να στεγάσετε ένα website στον υπολογιστή σας. Το web sharing δεν σας επιτρέπει να μοιράζεστε αρχεία και φακέλους στην ιστοσελίδα σας, αλλά χρήστες στο δίκτυο θα μπορούν να την αναγνώσουν. Αυτό είναι χρήσιμο όταν κατασκευάζετε μια ιστοσελίδα και θέλετε δοκιμαστικά να την μοιραστείτε με τρίτους.

Υπάρχουν δύο διαφορετικές ιστοσελίδες διαθέσιμες για τους χρήστες. Οι χρήστες μπορούν να δουν μόνο την ιστοσελίδα που είναι αποθηκευμένη στο /shortname/Sites φάκελο αν έχετε πρόσβαση στον υπολογιστή : http://your.computer.address/~yourusername/.

Με την χρήση του Web Sharing αποκαλύπτετε το όνομα χρήστη του λογαριασμού σας. Αυτό μπορεί να αποτελέσει διαρροή κρίσιμής πληροφορίας και πιθανή εκμετάλευσής της από κακόβουλους χρήστες. Η ακόλουθη ιστοσελίδα βρίσκεται στο Library/WebServer/Documents κατάλογο και είναι διαθέσιμη όταν η υπηρεσία Web Sharing είναι ενεργή : http://your.computer.address.



Εικόνα 60 - Επιλογές Web Sharing

Η υπηρεσία Web Sharing ως προεπιλογή είναι απενεργοποιημένη και θα πρέπει να παραμείνει έτσι αν δεν είναι απαραίτητο να χρησιμοποιηθεί. Αυτό αποτρέπει μη εξουσιοδοτημένους χρήστες από το να έχουν πρόσβαση στον υπολογιστή σας.

3.5. Τελικά συμπεράσματα

Ύστερα από την μεταστροφή του παλαιού λειτουργικού συστήματος της Apple σε ένα νέο όπου έχει σαν βάση το UNIX, το OS X υπέστη τεράστιες αλλαγές σε σχέση με τον προκάτοχό του. Ως προεγκατεστημένο και δίχως αλλαγές στις προεπιλεγμένες του ρυθμίσεις είναι ένα από τα καλύτερα θωρακισμένα λειτουργικά συστήματα UNIX. Παρόλα αυτά, ο διαχειριστής του συστήματος μπορεί να κάνει αλλαγές για να ασφαλίσει το σύστημα ακόμα περισσότερο. Το παρόν κείμενο παρουσίασε ένα πλήθος μεθόδων για να ασφαλίσουμε το Mac OS X σε τοπικό αλλά και δικτυακό επίπεδο.

4. Εξασφάλιση των Προσωπικών μας Πληροφοριών Μέσω των Κυριότερων Εφαρμογών

Χρησιμοποιούμε αυτό το κεφάλαιο για να ορίσουμε τις σωστές ρυθμίσεις για δικτυακές εφαρμογές και να θωρακίσουμε την ασφάλεια του δικτύου.

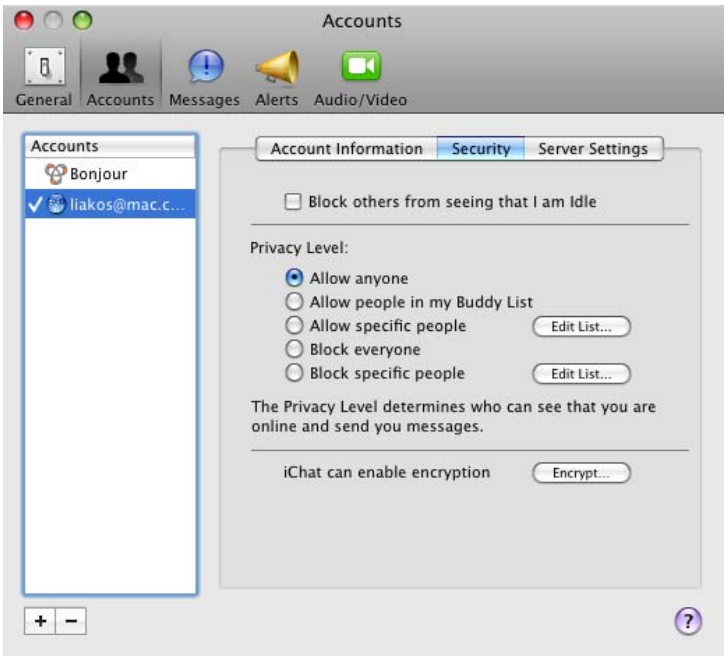
Η σωστή ρύθμιση των παραμέτρων για τις δικτυακές εφαρμογές είναι ένα σημαντικό βήμα στην θωράκιση του δικτύου μας από εξωγενείς επιθέσεις. Οργανισμοί βασίζονται σε δικτυακές υπηρεσίες για να επικοινωνήσουν με άλλους υπολογιστές σε ιδιωτικά δίκτυα (LAN) και δίκτυα εκτεταμένης κάλυψης (WAN). Απορυθμισμένες υπηρεσίες δικτύου αποτελούν ευκαιρίες για επίθεση από κακόβουλους χρήστες.

Παρόλο που οι εφαρμογές της Apple είναι εξ΄ ορισμού τους ασφαλείς, μπορούμε να βελτιώσουμε την ασφάλειά τους κάνοντας χρήση των παρακάτω πληροφοριών.

4.1.iChat

Μπορείτε να χρησιμοποιήσετε το iChat για να στείλετε με ασφάλεια κείμενο, ήχο και εικόνα. Μπορεί επίσης να χρησιμοποιηθεί για να αποστείλετε και αρχεία.

Για να ρυθμίσετε την εφαρμογή iChat, πρέπει εσείς και ο άλλος χρήστη να έχετε λογαριασμό στην online υπηρεσία .Mac[30] ή MobileMe και εγκατεστημένο ως λειτουργικό, μία έκδοση του OSX από την 10.4.3 και ύστερα. Με την συγκεκριμένη υπηρεσία μπορείτε να επιλέξετε ένα πιστοποιητικό ασφαλούς επικοινωνίας[31] μεταξύ της εφαρμογής.



Εικόνα 61 – Παράθυρο Ρυθμίσεων iChat

[30] Έχει μετονομαστεί σε Mobileme.com

[31] http://docs.info.apple.com/article.html?path=Mac/10.5/en/9089.html

Όταν κάνετε την παραπάνω επιλογή, το iChat πραγματοποιεί μία Αίτηση Ψηφιακού Πιστοποιητικού (Certificate Signing Request "CSR") στην υπηρεσία .Mac και επιστρέφει ένα πιστοποιητικό με το δημόσιο και ιδιωτικό κλειδί. Η ζεύξη (pair) δημοσίου και ιδιωτικού κλειδιού πραγματοποιείται κατά την διαδικασία του CSR.

Η κωδικοποίηση του iChat χρησιμοποιεί την τεχνική PKI (Public Key Infrastructure) . Τα δημόσια και ιδιωτικά ασύμμετρα κλειδιά προέρχονται από την ταυτότητα του .Mac χρήστη, όπου αποτελεί το πιστοποιητικό και ιδιωτικό κλειδί του χρήστη. Το ιδιωτικό κλειδί και το πιστοποιητικό αντιπροσωπεύουν την .Mac ταυτότητα. Αυτά τα κλειδιά χρησιμοποιούνται για να κωδικοποιήσουν συνομιλίες μεταξύ εσάς και του φίλου σας.

Όταν αποστέλνετε με κωδικοποίηση ένα μήνυμα, το iChat απαιτεί από τον παραλήπτη του μηνύματος το δικό του δημόσιο κλειδί. Στην συνέχεια κωδικοποιεί το μήνυμα βασιζόμενο στο συγκεκριμένο κλειδί. Μετά στέλνει το κωδικοποιημένο μήνυμα στον φίλο σας, όπου με την σειρά του το αποκωδικοποιεί με το ιδιωτικό του κλειδί.

Αν και σε γενικά πλαίσια το iChat είναι μία πολύ ασφαλής εφαρμογή, καλό θα ήταν ανάλογα με τις απαιτήσεις σας (εταιρικός ή οικιακός υπολογιστής), η υπηρεσία σύντομων μηνυμάτων να απενεργοποιείται τελείως. Άν υπάρχει iChat server, τότε υπάρχει η δυνατότητα ο χρήστης να δημιουργήσει μία ασφαλής σύνδεση με τον server και να ασφαλίσει την συνομιλία του. Καλό θα ήταν οι συνομιλίες να περιοριστούν μόνο σε άτομα που είναι γνωστά και εμπιστοσύνης, προκειμένου να αποφευχθούν οι περιπτώσεις "ψαρέματος" (phishing) για πληροφορίες.

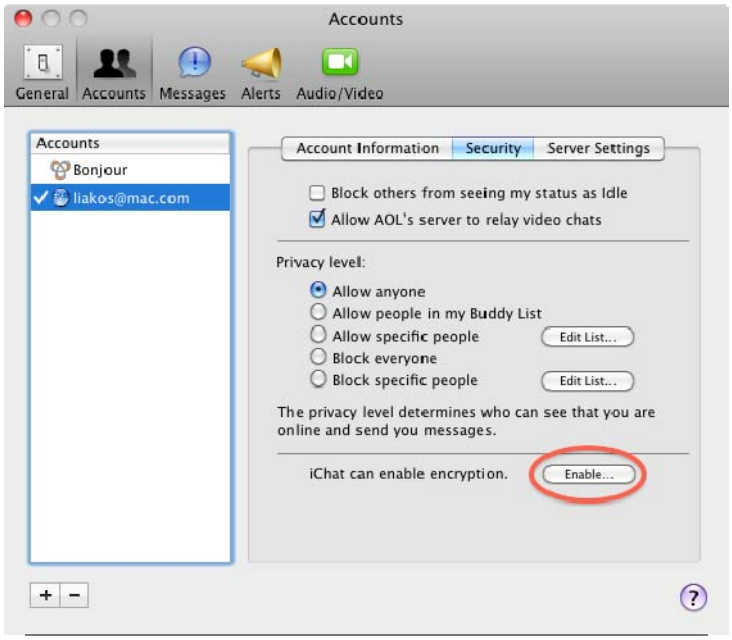
4.1.1. iChat AV Security

Όταν μοιράζεστε την οθόνη με έναν φίλο σας στο iChat, τότε εκείνος έχει τις ίδιες δυνατότητες πρόσβασης στον υπολογιστή σας που έχετε και εσείς. Μοιραστείτε τον Mac σας μόνο σε έμπιστα άτομα και να είστε ιδιαίτερα επιφυλακτικοί όταν σας στέλνουν προσκλήσεις άτομα που δεν είναι στην λίστα σας.

Εικόνα 62 – Παράδειγμα iChat AV

Άν η αίτηση για διαμοιρασμό έρχεται από κάποιον που είναι στην λίστα Bonjour, να έχετε υπ' όψη σας ότι το όνομά του δεν είναι απαραίτητα ακριβές, οπότε και η ταυτότητά του είναι αβέβαιη. Αν και κάθε σύνδεση διαμοιρασμού οθόνης χρησιμοποιεί κωδικοποίηση, το μεγαλύτερο επίπεδο ασφάλειας απαιτεί και οι δύο συμμετέχοντες να έχουν λογαριασμό .Mac ή MobileMe με την κωδικοποίηση ενεργοποιημένη. Αν ισχύει κάτι τέτοιο, θα υπάρχει η ένδειξη του λουκέτου στο παράθυρο του διαμοιρασμού. Για να τερματίσετε μία τέτοια συνεδρία, πατήστε Control-Escape.

Το iChat AV από το OS X v10.4.3 και ύστερα κωδικοποιεί όλες τις επικοινωνίες μεταξύ .Mac χρηστών. Κείμενα, ήχος, βίντεο και αρχεία είναι ασφαλισμένα με την χρήση 128 bit κωδικοποίησης ώστε κανείς ξένος να μην έχει πρόσβαση σε αυτά.



Εικόνα 63 – Επιλογές ασφάλειας iChat

Αν έχετε έναν ενεργό, πληρωμένο λογαριασμό .Mac ή MobileMe, μπορείτε να ρυθμίσετε το iChat να αποστέλλει τα δεδομένα σας κωδικοποιημένα σε άλλους χρήστες που έχουν ενεργοποιήσει την κωδικοποίηση στο iChat.

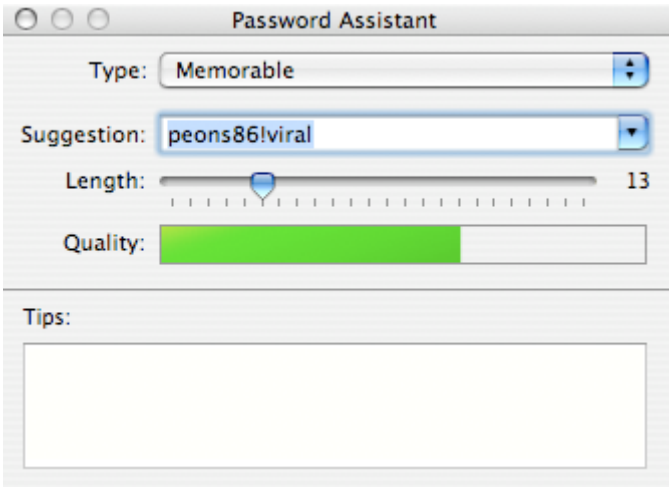
4.2.iTunes

Ο λογαριασμός iTunes που έχετε, προστατεύεται από το όνομα χρήστη και τον κωδικό σας, όπου ποτέ δεν πρέπει να τον μοιράζεστε με άλλους χρήστες, για να αποτρέψετε το ενδεχόμενο πρόσβασής του από τρίτους. Αν ένας μη εξουσιοδοτημένος χρήστης αποκτήσει πρόσβαση στον λογαριασμό σας, τότε αυτός έχει την δυνατότητα να αγοράσει τραγούδια, τηλεοπτικά σήριαλ και κινηματογραφικές ταινίες από το online κατάστημα του iTunes.

Εικόνα 64 - iTunes

Μπορείτε να αποτρέψετε τον λογαριασμό σας από το να "σπάσει", αν κάνετε την χρήση ενός ισχυρού κωδικού. Όταν έρθει η στιγμή να δημιουργήσετε τον κωδικό

σας στο iTunes, μπορείτε να κάνετε χρήση του εργαλείου Password Assistant προκειμένου να σας βοηθήσει να κατασκευάσετε έναν ισχυρό κωδικό.



Εικόνα 65 – Παράθυρο Εισαγωγής Κωδικού στο iTunes

Μπορείτε επίσης να χρησιμοποιήσετε την καρτέλα sharing στις ρυθμίσεις του iTunes για να μοιράσετε την μουσική σας βιβλιοθήκη και με άλλους χρήστες στο τοπικό σας δίκτυο. Όταν κάνετε χρήση αυτής της δυνατότητας, καλό θα ήταν η χρήση ενός ισχυρού κωδικού πρόσβασης για τους χρήστες που θέλουν να προσπελάσουν τα τραγούδια. Όπως και προηγουμένως, η χρήση του Password Assistant είναι επιτακτική.

Εικόνα 66 – Παράθυρο Ρυθμίσεων Κοινής Χρήσης Μουσικής Βιβλιοθήκης

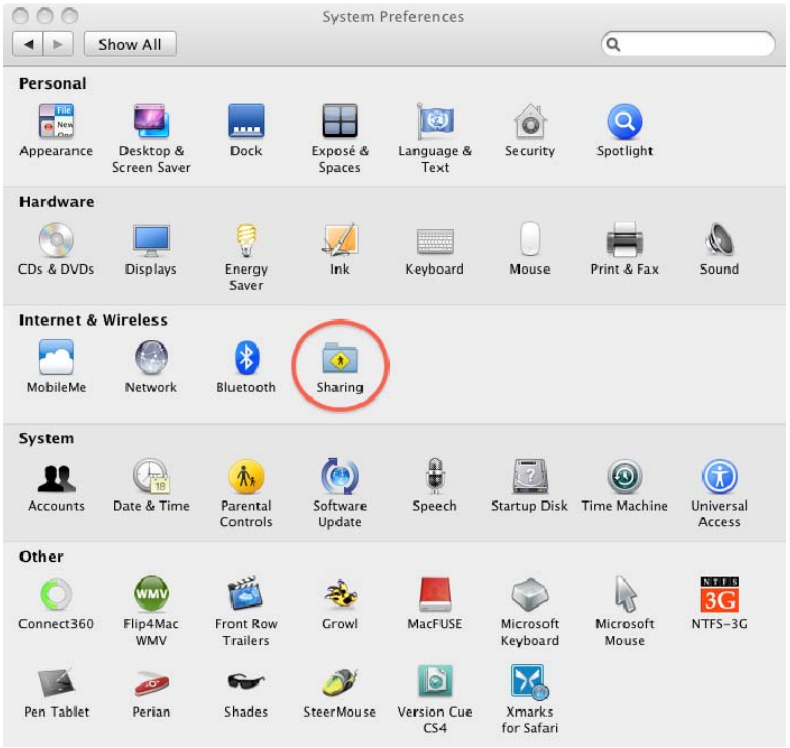
4.3.Firewall

4.3.1. Γενικά

Κατ' αρχάς, κάθε εφαρμογή firewall είναι σχεδιασμένη ώστε να ελέγχει την κίνηση στο δίκτυο από και προς τον υπολογιστή μας. Έρχεται προεγκατεστημένη σε κάθε διανομή του OS X και ο σκοπός της είναι να μας προστατεύσει από κακόβουλες εξωγενείς, αλλά και εσωγενείς, επιθέσεις στον υπολογιστή μας. Όπως κάθε εφαρμογή στο Mac OSX , έτσι και το firewall είναι σχεδιασμένο να είναι ταυτόχρονα εύχρηστο αλλά και πανίσχυρο στη λειτουργία του.

4.3.2. Συγκεκριμένες λειτουργίες

Μέσα από αυτό, ο χρήστης μπορεί να διαχειριστεί τις υπηρεσίες που απαιτούν πρόσβαση στο δίκτυο και ανάλογα να τους επιτρέψει ή να απαγορεύσει την προσβασιμότητα. Μέσα από την καρτέλα του System Preferences επιλέγουμε το Sharing.



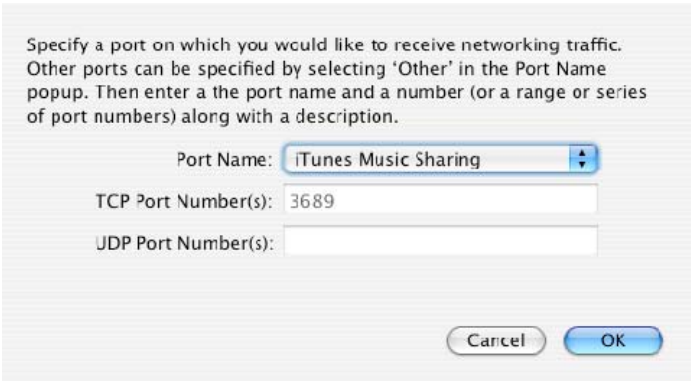
Εικόνα 67 - Παράθυρο Ρυθμίσεων Συστήματος

Από εκεί, επιλέγουμε το Tab Firewall και μας παρουσιάζεται το παρακάτω παράθυρο.

Εικόνα 68 - Παράθυρο Ρυθμίσεων Firewall

Μέσα από εκεί μπορούμε να κάνουμε τις βασικές μας ρυθμίσεις. Μπορούμε κατ' αρχάς να ενεργοποιήσουμε ή να απενεργοποιήσουμε γενικά την υπηρεσία του firewall. Επίσης μας δίνεται και μία λίστα από λειτουργίες που απαιτούν από τον υπολογιστή μας πρόσβαση στο δίκτυο. Οι περισσότερες είναι κοινές για όλα τα λειτουργικά συστήματα (π.χ. FTP), ενώ ορισμένες αφορούν μόνο υπολογιστές της συγκεκριμένης οικογένειας (π.χ. Bonjour). Το βασικό είναι ότι μπορούμε να παραμετροποιήσουμε τις ήδη υπάρχουσες ή ακόμα και να δημιουργήσουμε δικές μας.

Παραδείγματος χάρη, αν επιλέξουμε την υπηρεσία iTunes Music Sharing και κάνουμε Edit..., τότε μας παρουσιάζεται το παρακάτω παράθυρο , όπου μπορούμε μέσω ενός drop down menu να επιλέξουμε προκαθορισμένες ports ώστε να είναι ελεύθερη η πρόσβαση από και προς αυτές.



Εικόνα 69 – Προχωρημένες ρυθμίσεις Firewall

Σε περίπτωση που το port που θέλουμε δεν βρίσκεται στη λίστα, μπορούμε μόνοι μας, μέσω της επιλογής other. να καθορίσουμε το όνομα και τον αριθμό των ports που μας ενδιαφέρουν.

Πολύ ενδιαφέρουσα είναι και η επιλογή Advanced, όπου όταν την επιλέξουμε, παρουσιάζεται το παρακάτω παράθυρο :

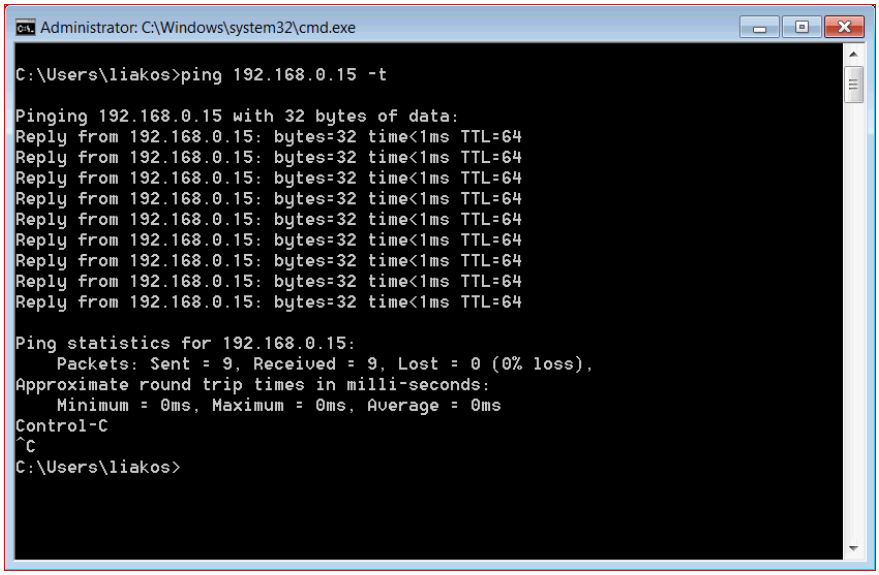
Εικόνα 70 - Παράθυρο Ρυθμίσεων Ports για το Firewall

Στη πρώτη επιλογή, το UDP (User Datagram Protocol) είναι ένα πρωτόκολλο επικοινωνίας που προσφέρει ένα περιορισμένο μέγεθος υπηρεσίας όταν τα μηνύματα ανταλλάσσονται μεταξύ των υπολογιστών που χρησιμοποιούν το Internet Protocol (IP). Όπως και το TCP, έτσι και το UDP χρησιμοποιεί το Internet Protocol για να πάρει μία μονάδα πληροφορίας (datagram), από τον έναν υπολογιστή στον άλλο. Δυστυχώς, αντίθετα με το TCP, το UDP δεν παρέχει υπηρεσία ώστε να διαχωρίζει τα πακέτα πληροφορίας σε μικρότερα κομμάτια (datagrams), και να τα ενώνει στο προορισμό του. Το UDP είναι ένα πρωτόκολλο προορισμένο περισσότερο στη συνεχή μεταφορά δεδομένων, όπου η παράδοση και η επιβεβαίωση δεν είναι εξασφαλισμένη. Με το να περιορίζουμε την κίνηση μέσα από το πρωτόκολλο UDP, αυξάνουμε την ασφάλεια του υπολογιστή μας.

Στη δεύτερη επιλογή, ορίζουμε ένα log file, δηλαδή ένα ιστορικό με τις περιπτώσεις όπου χρειάστηκε να επέμβει το firewall. Αυτό είναι ιδιαίτερα χρήσιμο αν θελήσουμε να εντοπίσουμε πιθανούς εισβολείς ή κακόβουλους χρήστες του υπολογιστή μας.

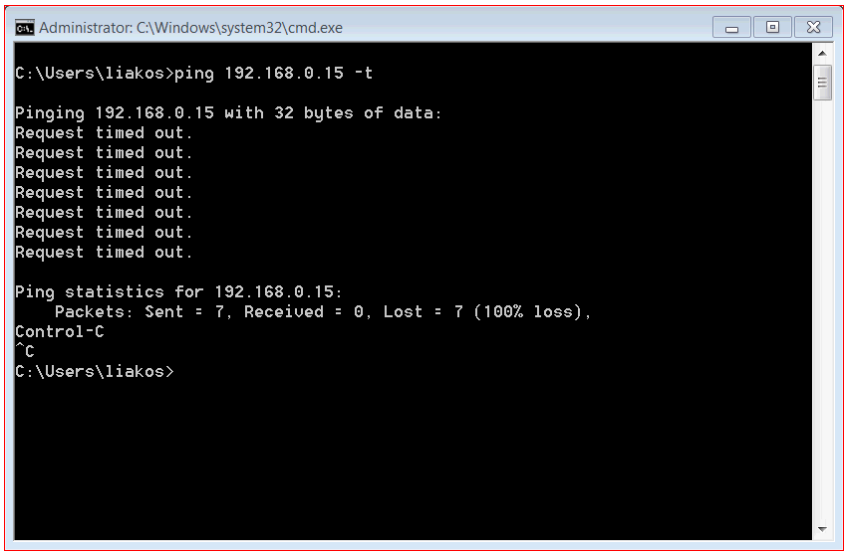
Η τρίτη επιλογή είναι και η περισσότερο ενδιαφέρουσα. Μέσα από αυτή μπορούμε να κάνουμε τον υπολογιστή αόρατο στις διαδικτυακές επιθέσεις. Όταν ενεργοποιήσουμε το Stealth Mode, όλη η ανεπιθύμητη κίνηση δεδομένων μέσα στο δίκτυο μας δεν λαμβάνει καμία απάντηση από τον υπολογιστή μας. Το Stealth mode κυριολεκτικά κρύβει τον υπολογιστή μας πίσω από το firewall, και οι άλλοι υπολογιστές που στέλνουν κίνηση στον δικό μας, δεν λαμβάνουν καμία πληροφορία σχετικά με τον υπολογιστή μας.

Στην παρακάτω εικόνα ο υπολογιστής Mac έχει την διεύθυνση IP 192.168.0.11 και του κάνουμε Ping από έναν υπολογιστή με Windows Vista. Τα αποτελέσματα είναι τα παρακάτω και είναι αναμενόμενα.



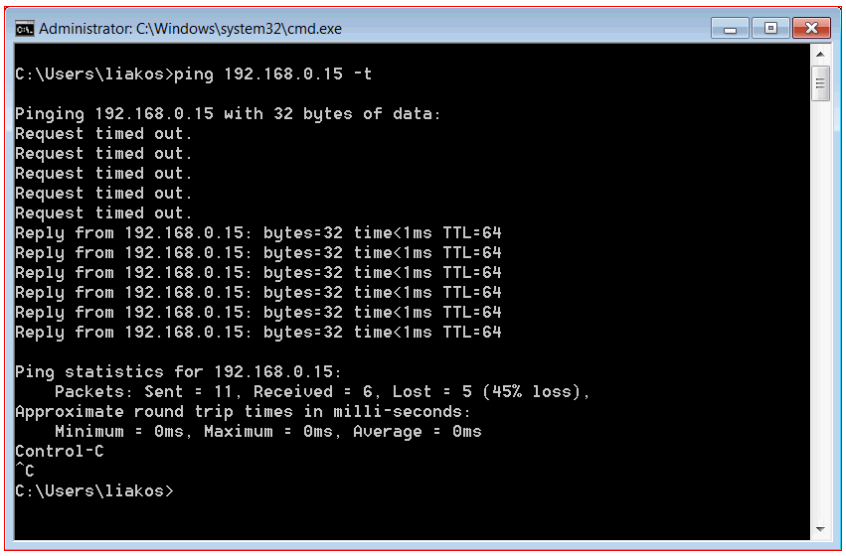
Εικόνα 71 – Stealth mode απενεργοποιημένο

Στη συνέχεια ενεργοποιούμε το Stealth mode στον Mac υπολογιστή και τα αποτελέσματα είναι τα παρακάτω :



Εικόνα 72 – Stealth mode ενεργοποιημένο

Τέλος, για να δείξουμε την αμεσότητα και αποτελεσματικότητα της υπηρεσίας αυτής, ενεργοποιούμε και απενεργοποιούμε το Stealth mode όταν το Windows based μηχάνημα μας κάνει Ping :



Εικόνα 73 – Stealth mode στην αρχή ενεργοποιημένο και στην συνέχεια απενεργοποιημένο

Με τα παραπάνω είναι εμφανές ότι το Stealth mode είναι ένα εξαιρετικά χρήσιμο εργαλείο στη θωράκιση του υπολογιστή μας από δικτυακές επιθέσεις και αδιάκριτα βλέμματα.

4.4.Mail

Μπορούμε να αλλάξουμε τις επιλογές της εφαρμογής Mail, έτσι ώστε να ενισχύσουμε την παρεχόμενη ασφάλεια. Ανάλογα με τις ρυθμίσεις του mail server που έχουμε επιλέξει, μπορούμε να ενεργοποιήσουμε την χρήση SSL και Kerberos-based πιστοποίηση ταυτότητας. Αυτές οι ρυθμίσεις πρέπει να υποστηρίζονται από τον mail server προκειμένου να τις αξιοποιήσουμε

Να στέλνουμε mail που είναι υπογεγραμμένο ψηφιακά και κωδικοποιημένο Ψηφιακά κωδικοποιημένα μηνύματα αφήνουν τους παραλήπτες να επιβεβαιώσουν την ταυτότητα του αποστολέα και προσφέρουν την εξασφάλιση ότι το μήνυμα δεν αλλοιώθηκε κατά την μεταφορά. Κωδικοποιημένα μηνύματα κρατούν τα δεδομένα τους κρυφά και είναι προσβάσιμα μόνο από τον επιλεγμένο παραλήπτη.

Μπορούμε να στείλουμε κωδικοποιημένα μηνύματα σε παραλήπτες αν έχουμε παραλάβει ένα ψηφιακά υπογεγραμμένο μήνυμα από εκείνους ή αν έχουμε πρόσβαση στο δημόσιο κλειδί τους. Οι παραλήπτες λαμβάνουν το δημόσιο κλειδί μας μόλις λάβουν το υπογεγραμμένο μήνυμά μας.

Το συγκεκριμένο σύστημα πιστοποίησης αναφέρεται ως σύστημα διανομής δημοσίου κλειδιού ‘public key infrastructure (PKI)’. Εξασφαλίζει ότι το μήνυμα είναι από τον συγκεκριμένο αποστολέα και δεν αλλοιώθηκε κατά την μεταφορά. Όταν χρησιμοποιούμε την μέθοδο PKI και κωδικοποιούμε το μήνυμα τότε είμαστε σίγουροι ότι μόνο ο επιθυμητός παραλήπτης μπορεί να διαβάσει και να προσπελάσει τα περιεχόμενα.

Η εφαρμογή Mail αναγνωρίζει τα πιστοποιητικά του αποστολέα και του παραλήπτη. Σε ενημερώνει για την παρουσία πιστοποιητικού στο μήνυμα με ένα εικονίδιο θαυμαστικού και την κωδικοποίηση με ένα εικονίδιο λουκέτου. Όταν στέλνεις υπογεγραμμένο ή κωδικοποιημένο ένα μήνυμα, το πιστοποιητικό του αποστολέα πρέπει να περιλαμβάνει την case-sensitive διεύθυνση από τα περιεχόμενα διευθύνσεων του Mail.app.

Για περαιτέρω ασφάλεια μπορούμε να απενεργοποιήσουμε την εμφάνιση απομακρυσμένων εικόνων στα μηνύματα. Οι αποστολείς μαζικών emails χρησιμοποιούν μηχανισμούς αναγνώρισης για το αν ο παραλήπτης βλέπει τις εικόνες που του στέλνουν. Αν δεν ανοίγουμε τις εικόνες που μας στέλνουν , τότε περιορίζουμε το φαινόμενο του spam-mail.

4.4.1. Ενεργοποιώντας το Account Security

Μπορούμε να ρυθμίσουμε την εφαρμογή Mail.App να στέλνει και να δέχεται ασφαλή μηνύματα χρησιμοποιώντας το πρωτόκολλο SSL για να εγκαθιδρύσει μια ασφαλή σύνδεση με τον mail server. Στο Mac OSX v10.5 υπάρχει υποστήριξη για SSLv2, SSLv3, και TLSv1. Το SSL αποτρέπει άλλους χρήστες στο να έχουν πρόσβαση στην επικοινωνία και να αποκτούν μη εξουσιοδοτημένη πρόσβαση στα δεδομένα μας.

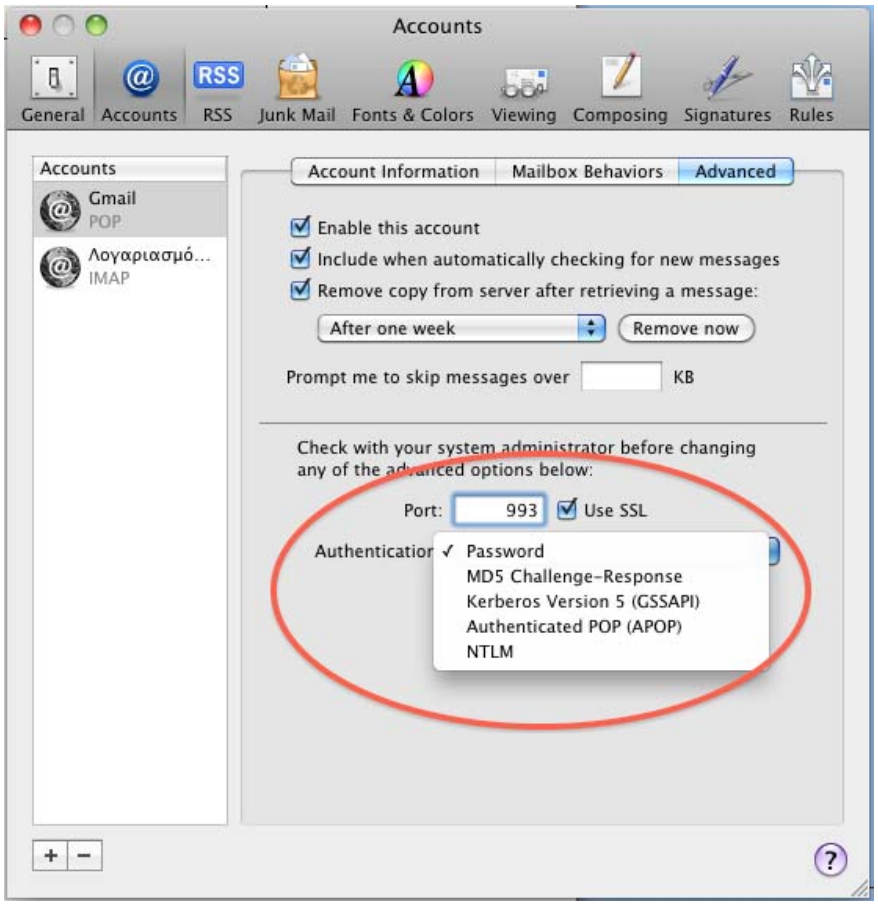
Αν χρησιμοποιείς SSL για να συνδεθείς στον mail server , ο κωδικός σου και τα δεδομένα σου μεταφέρονται με ασφάλεια. Επιπρόσθετα όμως, μπορούμε να βελτιώσουμε την ασφάλεια του κωδικού με την χρήση μίας ισχυρής μεθόδου αυθεντικοποίησης. Μπορείς να προστατέψεις τον κωδικό με τις παρακάτω μεθόδους :

- MD5 Challenge-Response
- NTLM
- Kerberos Version 5 (GSSAPI)

4.4.2. Για να χρησιμοποιήσουμε μια ασφαλή σύνδεση με τον mail server

- Επιλέγουμε Mail>Preferences και μετά κάνουμε κλικ στο Accounts.
- Επιλέγουμε έναν λογαριασμό και μετά Advanced
- Επιλέγουμε την χρήση του SSL. Ο προεπιλεγμένος αριθμός πύλης είναι ο 993. Για να λειτουργήσει το πρωτόκολλο SSL, πρέπει να είναι ρυθμισμένο στην ίδια πύλη.
- Από το αναδυόμενο Authentication μενού, επιλέγουμε μία από τις ακόλουθες μεθόδους πιστοποίησης :
- MD5 Challenge-Response
- NTLM
- Kerberos Version 5 (GSSAPI)
- Επιλέγουμε το Account Information
- Από το μενού Outgoing Mail Server (SMTP) επιλέγουμε Edit Server List.
- Από την λίστα με τους servers, επιλέγουμε τον server της εξερχόμενης αλληλογραφίας και μετά Advanced.
- Επιλέγουμε Secure Socket Layer (SSL).

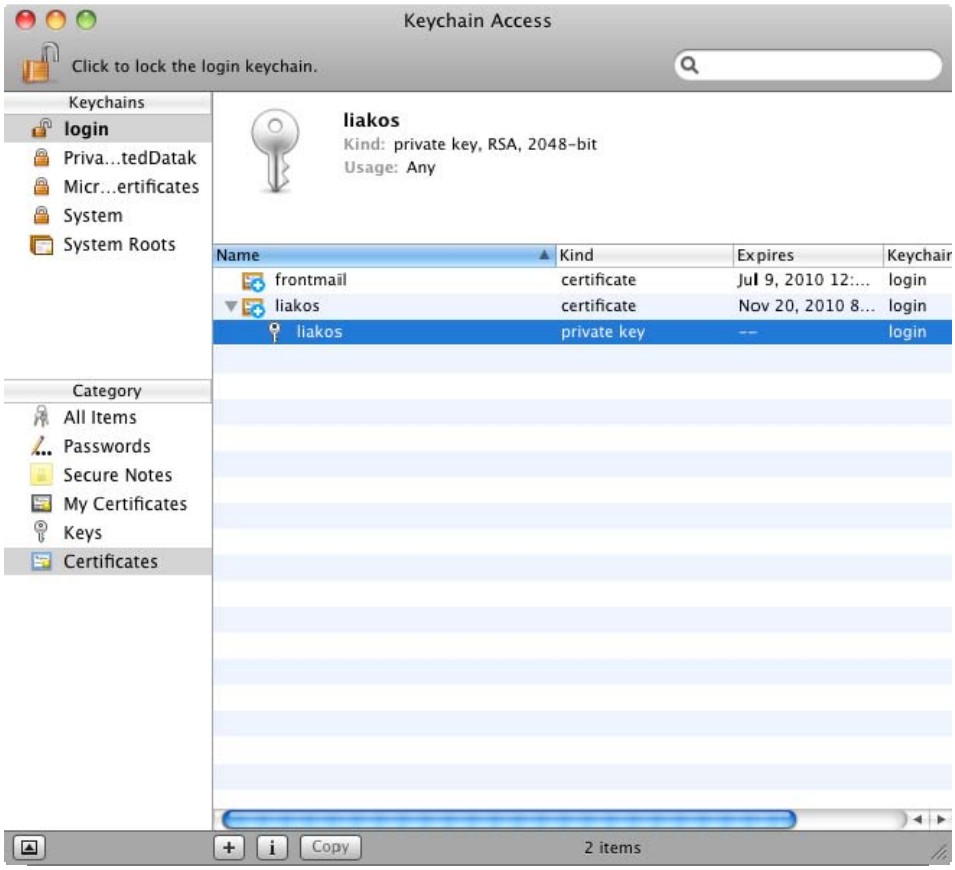
- Κλείνουμε το παράθυρο των επιλογών και στην συνέχεια επιλέγουμε save στο μήνυμα που μας παρουσιάζεται.



Εικόνα 74 – Setup λογαριασμού στο Mail App με ασφαλείς ρυθμίσεις

4.4.3. Υπογράφοντας και κωδικοποιώντας Ηλεκτρονικά Μηνύματα

Ένα υπογεγραμμένο μήνυμα (συμπεριλαμβανομένου και τις επισυνάψεις) επιτρέπει στον παραλήπτη να επιβεβαιώσει την ταυτότητά σου ως αποστολέα και παρέχει εξασφάλιση ότι το μήνυμα δεν αλλοιώθηκε κατά την μεταφορά. Για να στείλεις ένα υπογεγραμμένο μήνυμα, θα πρέπει να έχεις μία ψηφιακή υπογραφή στην κλειδοθήκη του συστήματος. Η ψηφιακή σου ταυτότητα είναι ένας συνδυασμός από προσωπικά πιστοποιητικά και το ανάλογο ιδιωτικό κλειδί. Μπορείς να δεις τις ψηφιακές ταυτότητες στην κλειδοθήκη, επιλέγοντας το Keychain Access και στην συνέχεια κάνοντας κλικ στο Certificates στην Category list.



Εικόνα 75 - Τα πιστοποιητικά

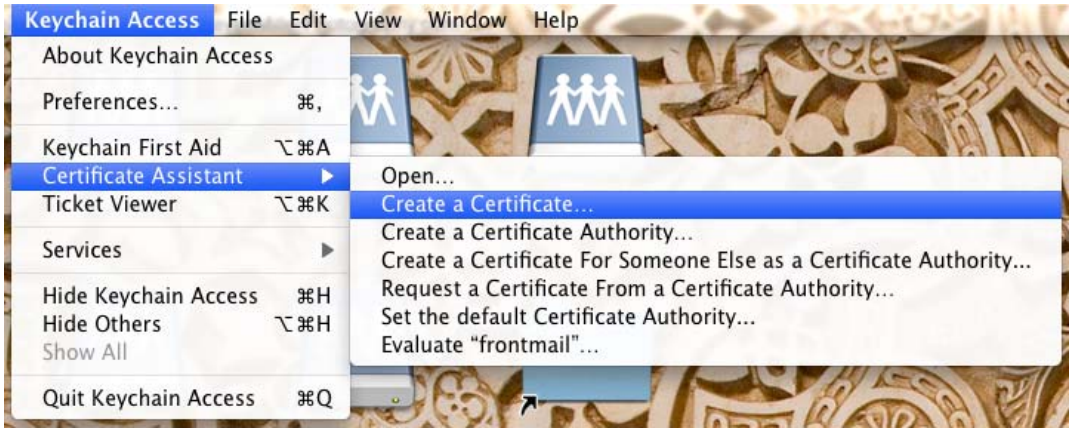
Αν έχεις μόνο το πιστοποιητικό αλλά σου λείπει το προσωπικό κλειδί, δεν μπορείς να στείλεις υπογεγραμμένα μηνύματα. Πρέπει να έχεις το ανάλογο προσωπικό κλειδί. Επίσης, αν υπάρχουν άτομα που χρησιμοποιούν το πιστοποιητικό σου για να στείλουν κωδικοποιημένα μηνύματα, πρέπει να έχεις εγκατεστημένο το προσωπικό σου κλειδί μέσα στον υπολογιστή που προσπαθείς να δεις το μήνυμα, διαφορετικά η ανάγνωσή του θα είναι αδύνατη.

Ένα κωδικοποιημένο μήνυμα (συμπεριλαμβανομένου και των επισυνάψεων) προσφέρει ένα μεγαλύτερο επίπεδο ασφάλειας από ένα υπογεγραμμένο ηλεκτρονικό μήνυμα. Για να στείλεις ένα κωδικοποιημένο μήνυμα, πρέπει να έχεις μία ψηφιακή ταυτότητα και το πιστοποιητικό του κάθε παραλήπτη πρέπει να είναι εγκατεστημένο στην εφαρμογή Keychain Access.

Για να κατασκευάσουμε μία ψηφιακή ταυτότητα ακολουθούμε τα παρακάτω βήματα :

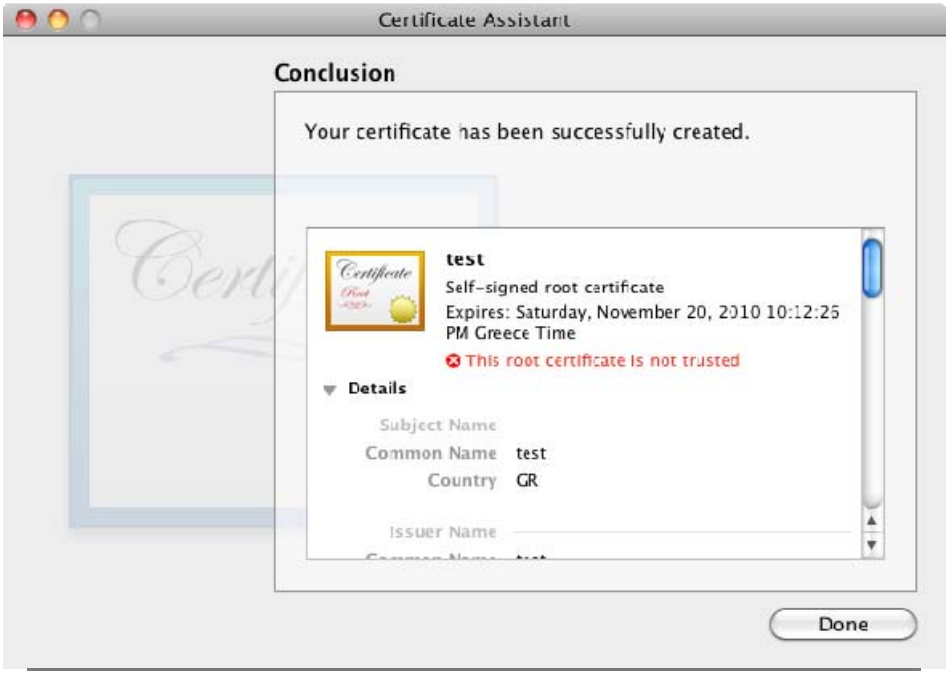
- Ξεκινάμε την εφαρμογή Keychain
- Επιλέγουμε Keychain Access > Certificate Assistant > Create Certificate
- Γράφουμε ένα όνομα

- Επιλέγουμε ένα Identity Type και στην συνέχεια επιλέγουμε τον τύπο του πιστοποιητικού
- Επιλέγουμε Continue
- Ελέγχουμε τις λεπτομέρειες και πατάμε Done



Εικόνα 76 - Επιλογή Wizard για δημιουργία ψηφιακής ταυτότητας

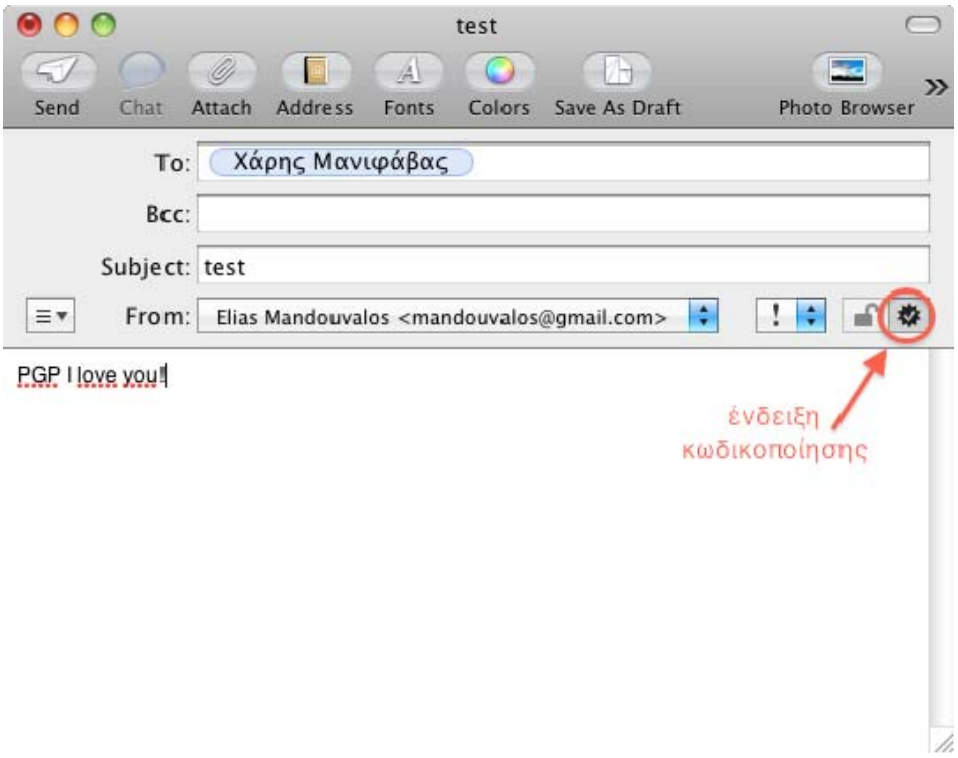
Εικόνα 77 - Ρυθμίσεις Πιστοποιητικού



Εικόνα 78 - Επισκόπηση λεπτομερειών πιστοποιητικού

4.4.4. Υπογραφή και κωδικοποίηση μηνύματος

1. Επιλέγεις File > New Message και στην συνέχεια τον λογαριασμό που επιθυμείς να στείλεις το μήνυμα. Ο συγκεκριμένος λογαριασμός πρέπει να έχει το προσωπικό του πιστοποιητικό εγκατεστημένο στην κλειδοθήκη σου. Κατά την σύνταξη του μηνύματος θα υπάρχει ένα ενδεικτικό εικονίδιο (ένα θαυμαστικό), όπου θα μας υπενθυμίζει ότι θα είναι υπογεγραμμένο όταν το αποστείλουμε.

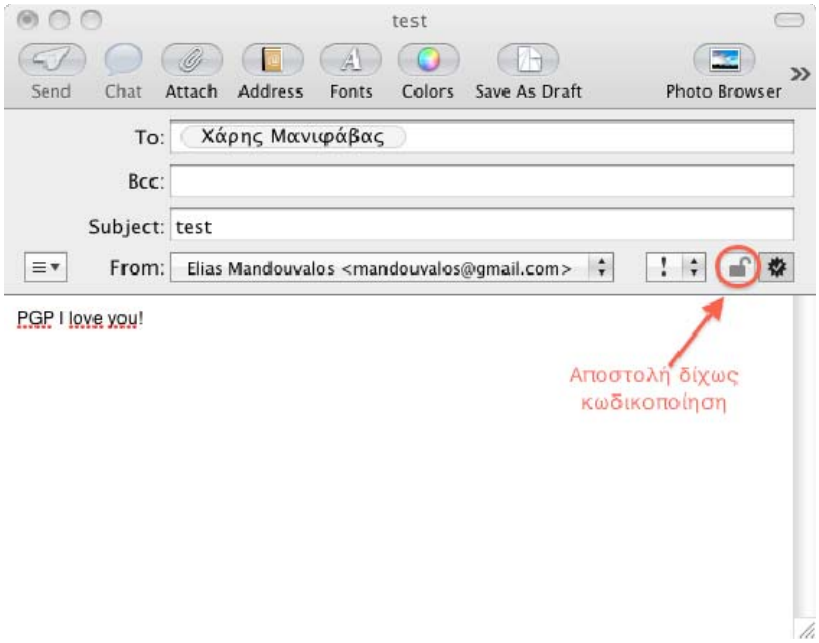


Εικόνα 79 - Ρυθμίσεις Secure Mail

2. Μεταφέρουμε το μήνυμα στους παραλήπτες. Αν στέλνουμε το μήνυμα σε μία λίστα με παραλήπτες (mailing list), καλύτερα θα ήταν να το στείλουμε χωρίς υπογραφή. Πολλές λίστες απορρίπτουν τα υπογεγραμμένα μηνύματα, γιατί η υπογραφή είναι μία επισύναψη. Για να στείλεις ένα μήνυμα ανυπόγραφο, κάνουμε κλικ στο εικονίδιο του θαυμαστικού. Ένα 'X' αντικαθιστά το θαυμαστικό.

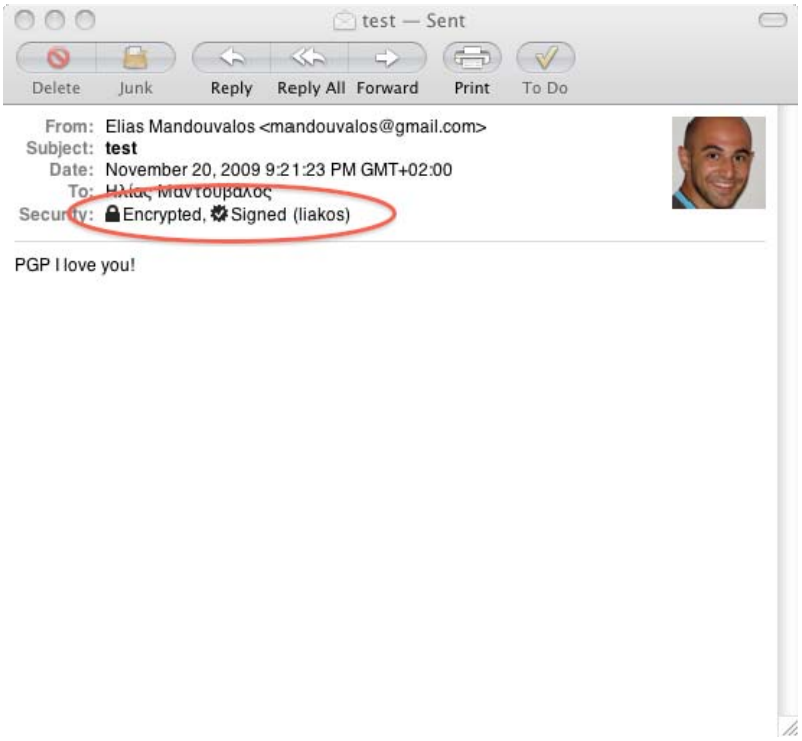
Το εικονίδιο της κωδικοποίησης (μία κλειστή κλειδαριά), εμφανίζεται δίπλα στο εικονίδιο της υπογραφής, αν έχεις το προσωπικό πιστοποιητικό του παραλήπτη μέσα στην κλειδοθήκη σου. Αυτό το εικονίδιο δείχνει ότι το μήνυμα θα κωδικοποιηθεί όταν το αποστείλουμε.

Αν δεν έχουμε όλα τα πιστοποιητικά των παραληπτών, θα μας ζητηθεί να ακυρώσουμε το μήνυμα ή να το στείλουμε δίχως κωδικοποίηση. Για να στείλουμε το μήνυμα αποκωδικοποιημένο, κάνουμε κλικ στο εικονίδιο της κωδικοποίησης. Ένα ανοιχτό λουκέτο αντικαθιστά το κλειστό.

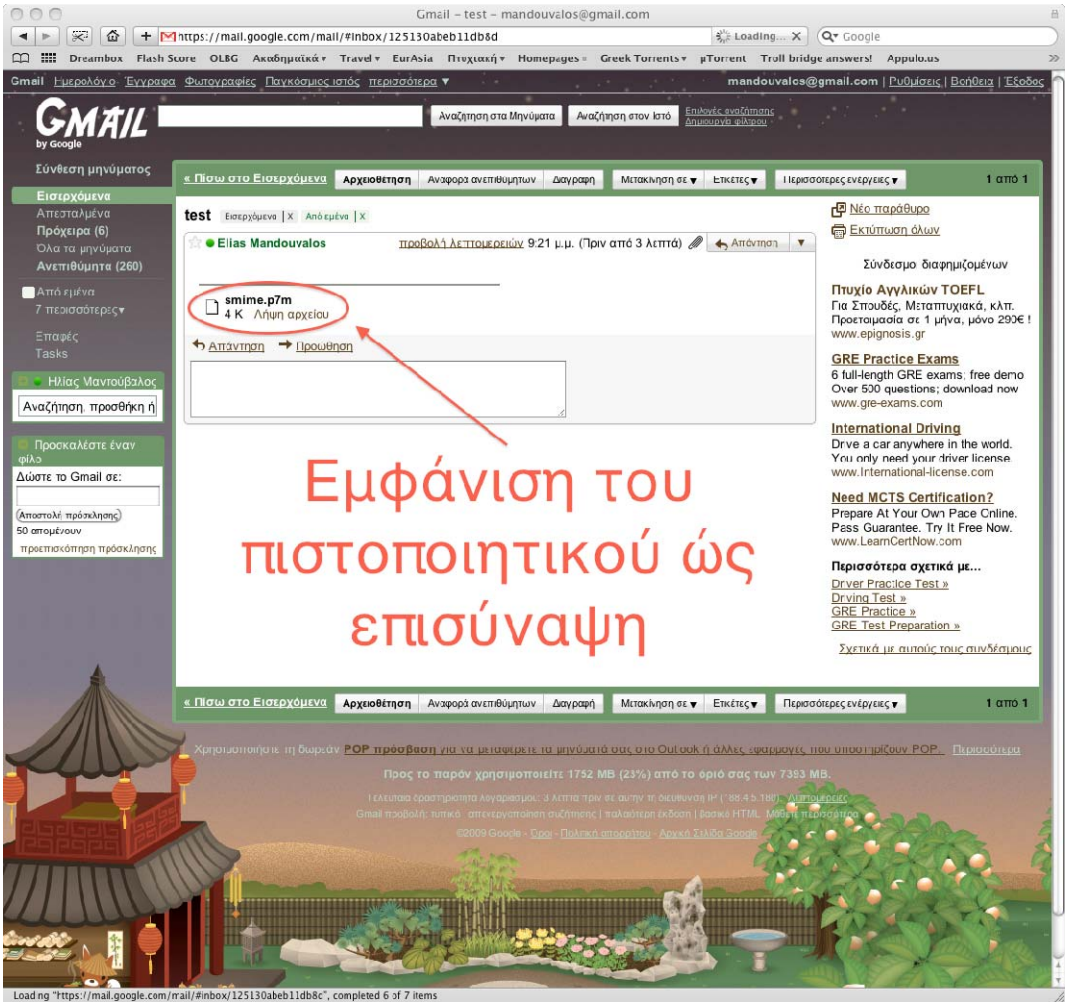


Εικόνα 80 - Ρυθμίσεις Mail χωρίς κωδικοποίηση

Αν οι παραλήπτες χρησιμοποιούν την εφαρμογή Mail τότε οι επικεφαλίδες των μηνυμάτων που θα παραλάβουν θα έχουν τις ενδείξεις της Κωδικοποίησης και της Υπογραφής. Αν χρησιμοποιούν μια εφαρμογή που δεν υποστηρίζει υπογεγραμμένα και κωδικοποιημένα μηνύματα, το πιστοποιητικό μπορεί να είναι στην μορφή επισύναψης. Αν οι παραλήπτες αποθηκεύσουν τις επισυνάψεις ως αρχεία, μπορούν να προσθέσουν το πιστοποιητικό σου στην κλειδοθήκη τους.



Εικόνα 81 - Λήψη ασφαλούς email από υποστηριζόμενη εφαρμογή



Εικόνα 82 - Λήψη ασφαλούς email από μη υποστηριζόμενη εφαρμογή

4.5.Safari

4.5.1. Ασφαλής Πλοήγηση

Μπορούμε να αλλάξουμε τις ρυθμίσεις της εφαρμογής Safari, προκειμένου να βελτιώσουμε την ασφάλειά του. Με τις κατάλληλες ρυθμίσεις μπορούμε να αποτρέψουμε πληροφορίες στον υπολογιστή μας από το να κινδυνέψουν ή να αποκαλυφθούν σε τρίτους.

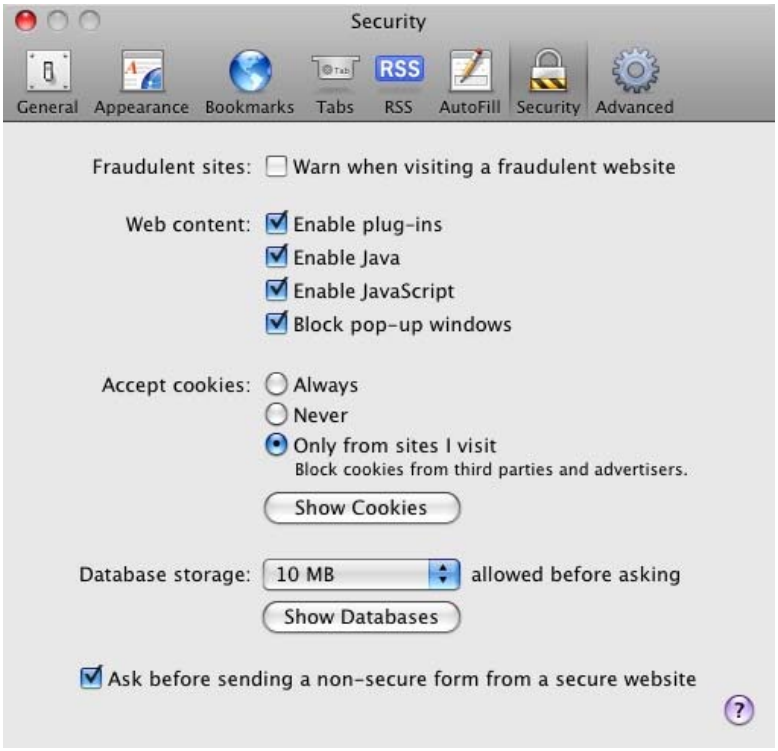
Συγκεκριμένα, οι ρυθμίσεις που μπορούμε να αλλάξουμε είναι : η απενεργοποίηση της αυτόματης συμπλήρωσης (AutoFill), το αυτόματο άνοιγμα αρχείων μετά το download, η απενεργοποίηση των cookies, της javascript και η ερώτηση πριν στείλουμε επισφαλείς φόρμες ερωτηματολογίου.

Μετά την απενεργοποίηση των cookies, θα πρέπει να διαγράψουμε τα υπάρχοντα cookies από την επιλογή που μας παρέχεται στο πλαίσιο security του browser. Για ιστοσελίδες που απαιτούν cookies, μπορούμε να τα ενεργοποιήσουμε προσωρινά.

Η χειροκίνητη ενεργοποίηση και απενεργοποίηση των cookies μπορεί να είναι χρονοβόρα αν επισκεπτόμαστε πολλές ιστοσελίδες που χρειάζονται την χρήση τους. Μία πιθανή λύση είναι η χρήση πολλαπλών λογαριασμών χρηστών με διαφορετικές επιλογές σχετικά με τα cookies. Για παράδειγμα, ο προσωπικός μας λογαριασμός μπορεί να επιτρέπει όλα τα cookies, ενώ ένας περισσότερο ασφαλής λογαριασμός χρήστη μπορεί να έχει αυστηρότερη ρύθμιση σχετικά με αυτό.

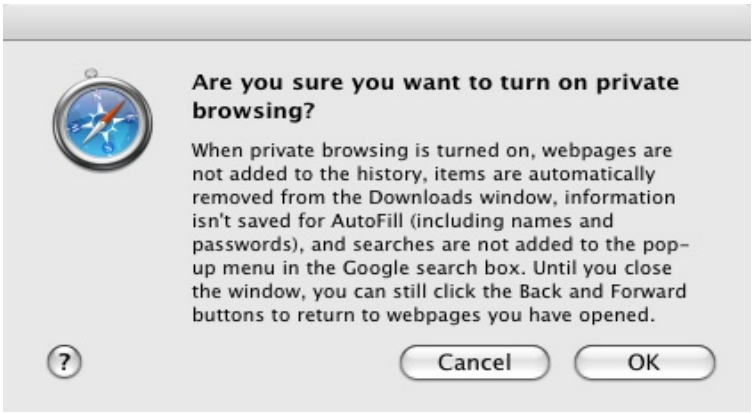
Η γλώσσα Javascript[32] έχει ενσωματωμένους περιορισμούς και αποτρέπουν τις εφαρμογές από το να βλάψουν τον υπολογιστή. Παρόλα αυτά, αν την απενεργοποιήσουμε, μπορούμε να ασφαλίσουμε ακόμα περισσότερο το σύστημά μας από μη εξουσιοδοτημένες εφαρμογές javascript που θέλουν να εκτελεστούν στον υπολογιστή μας.

[32] https://developer.mozilla.org/en/JavaScript



Εικόνα 83 - Παράθυρο Ρυθμίσεων Ασφάλειας Safari

Όταν χρησιμοποιούμε τον Safari, να κάνουμε χρήση της λειτουργίας που έχει για private browsing[33]. Η συγκεκριμένη λειτουργία αποτρέπει τον browser από το να καταγράφει λειτουργίες, να κρατά ιστορικό, να διατηρεί αντικείμενα στην λίστα Downloads , να αποθηκεύει στοιχεία για αυτόματη συμπλήρωση πεδίων και να διατηρεί ιστορικό για τις αναζητήσεις στο Google. Μπορούμε να χρησιμοποιήσουμε τα κουμπιά για μπρος και πίσω πλοήγηση, αλλά μόλις κλείσουμε το συγκεκριμένο παράθυρο, τότε το ιστορικό τους θα διαγραφεί.



Εικόνα 84 – Παράθυρο Ενεργοποίησης Ιδιωτικής Περιήγησης

Πίνακας 8 – Συγκριτικά Private Browsing

[33] https://wiki.mozilla.org/User:Mconnor/PrivateBrowsing

Ημερομηνία	Browser	Ονομασία
29 Απριλίου 2005	Safari 2.0	Private Browsing
11 Δεκεμβρίου 2008	Google Chrome 1.0	Incognito
19 Μαρτίου 2009	Internet Explorer 8	InPrivate
30 Ιουνίου 2009	Mozilla Firefox 3.5	Private Browsing

Παρατηρούμε ότι ο πρώτος browser που είχε την δυνατότητα για private browser ήταν ο Safari και μάλιστα αρκετά νωρίτερα από τους ανταγωνιστές του. Έκτοτε, σχεδόν όλοι έχουν υιοθετήσει αυτή την δυνατότητα, με διαφορετική ονομασία ο καθένας.

4.6. Time Machine

4.6.1. Κατανοώντας την αρχιτεκτονική του Time Machine.

Το σύστημα του Time Machine βασίζεται στο σύστημα αρχείων του Mac OS X HFS+[34]. Παρακολουθεί τις αλλαγές που συμβαίνουν στα αρχεία και τις τυχών αλλαγές στις άδειες πρόσβασης στο επίπεδο των χρηστών και των αρχείων.

Όταν το Time Machine δημιουργεί το αρχικό backup , αντιγράφει όλα τα περιεχόμενα του υπολογιστή στο εφεδρικό σκληρό δίσκο για να προστατέψει τα δεδομένα από μη εξουσιοδοτημένους χρήστες. Κάθε επόμενο backup βασίζεται πάνω στο αρχικό, που σημαίνει ότι αντιγράφει μόνο τις αλλαγές που συνέβησαν από το αρχικό backup.

Εικόνα 85 - Κεντρικό παράθυρο Time Machine

[34] http://developer.apple.com/mac/library/technotes/tn/tn1150.html

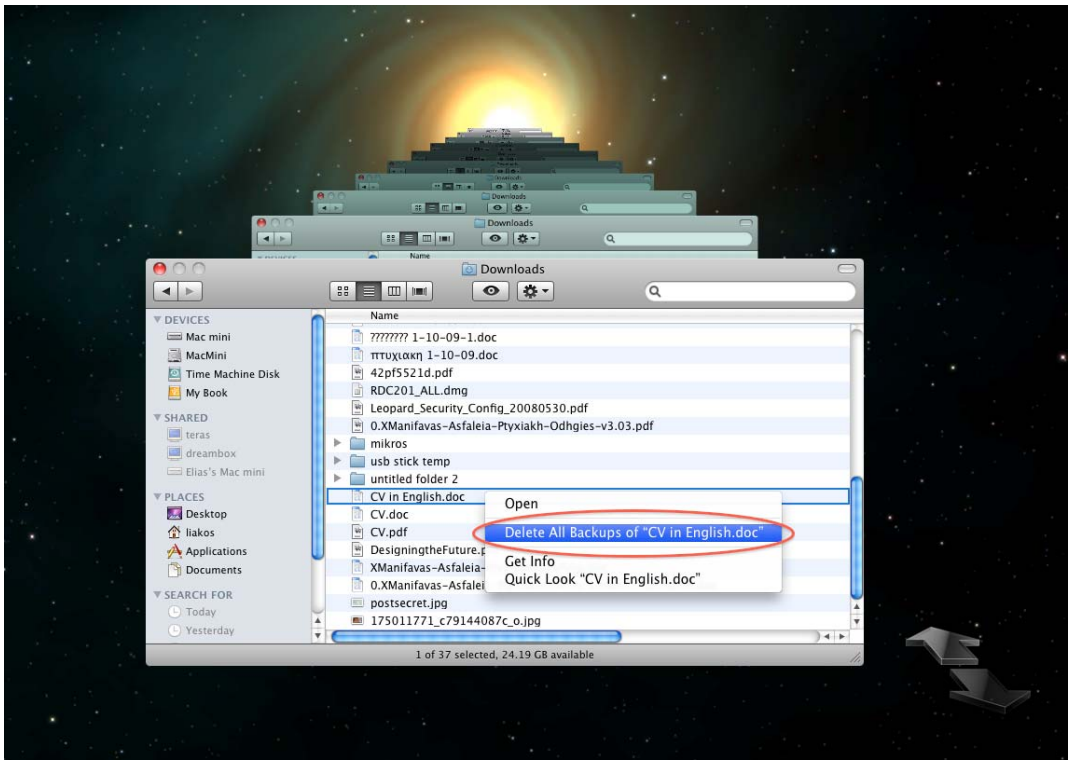
4.6.2. Διαγράφοντας μόνιμα τα αντίγραφα από το Time Machine

Μπορούμε να διαγράψουμε μόνιμα τα αρχεία ή τους φακέλους από τον υπολογιστή και τα Time Machine backups χρησιμοποιώντας το Time Machine. Αυτό αποτρέπει οποιοδήποτε παλιό και ευαίσθητο δεδομένο που δεν χρειαζόμαστε πλέον , να διαγραφεί οριστικά.

Για να διαγράψουμε μόνιμα αρχεία και φακέλους από το Time Machine :

- Διαγράφουμε το αρχείο ή τον φάκελο από τον υπολογιστή
- Ανοίγουμε το Time Machine
- Επιλέγουμε το αρχείο ή το φάκελο που θέλουμε να διαγράψουμε μόνιμα από το Time Machine
- Κάνουμε κλικ στο Action pop-up μενού και επιλέγουμε "Delete All Backups of "File or Folder name."
- Όταν το προειδοποιητικό μήνυμα εμφανιστεί, πατάμε OK για την μόνιμη διαγραφή του αρχείου ή φακέλου.

Όλα τα αντίγραφα ασφαλείας του αρχείου ή του φακέλου έχουν τώρα μόνιμα διαγραφεί από τον υπολογιστή.



Εικόνα 86 - Μόνιμη διαγραφή των Backups στο Time Machine

4.6.3. Αποθηκεύοντας Αντίγραφα μέσα σε Ασφαλή Αποθήκευση

Μπορούμε επίσης να αποθηκεύσουμε συγκεκριμένα αρχεία ή φακέλους που περιέχουν ευαίσθητα δεδομένα με το να τα τοποθετούμε σε μία εικόνα δίσκου με κωδικοποίηση. Στη συνέχεια αυτή η εικόνα πρέπει να τοποθετηθεί σε οποιαδήποτε server και μπορεί να ενημερώνεται κανονικά αλλά και να διατηρεί την ακεραιότητα των δεδομένων σας, εφόσον είναι προστατευμένη με κωδικοποίηση.

Για παράδειγμα, οι χρήστες Mac που είναι σε έναν Windows Server μπορούν να χρησιμοποιήσουν αυτή τη μέθοδο αποθήκευσης για να εξασφαλίσουν ότι ευαίσθητα δεδομένα τους είναι εξασφαλισμένα και ενημερωμένα.

Για να αποθηκεύσουμε και να κωδικοποιήσουμε τα δεδομένα μας :

1. Δημιουργούμε μία εικόνα δίσκου
2. Προσαρτούμε (mount) την εικόνα του δίσκου
3. Αντιγράφουμε τα αρχεία που θέλουμε να αποθηκεύσουμε στην εικόνα του δίσκου
4. Αποπροσαρτουμε (unmount) την εικόνα του δίσκου και την αντιγράφουμε στον εφεδρικό μας δίσκο

Αν είμαστε σε ένα περιβάλλον Windows Server, αντιγράφουμε την εικόνα του δίσκου μας σε ένα φάκελο που έχει αντίγραφα ασφαλείας των Windows Server. Τα δεδομένα σας τότε θα έχουν κωδικοποιηθεί και στην συνέχεια θα έχουν αποθηκευτεί.

4.6.4. Ανακτώντας Αντίγραφα δεδομένων από μία ασφαλή τοποθεσία

Αν από σφάλμα διαγράψουμε ή χάσουμε ένα αρχείο, μπορούμε να το ανακτήσουμε από το κωδικοποιημένο μας αντίγραφο ασφαλείας.

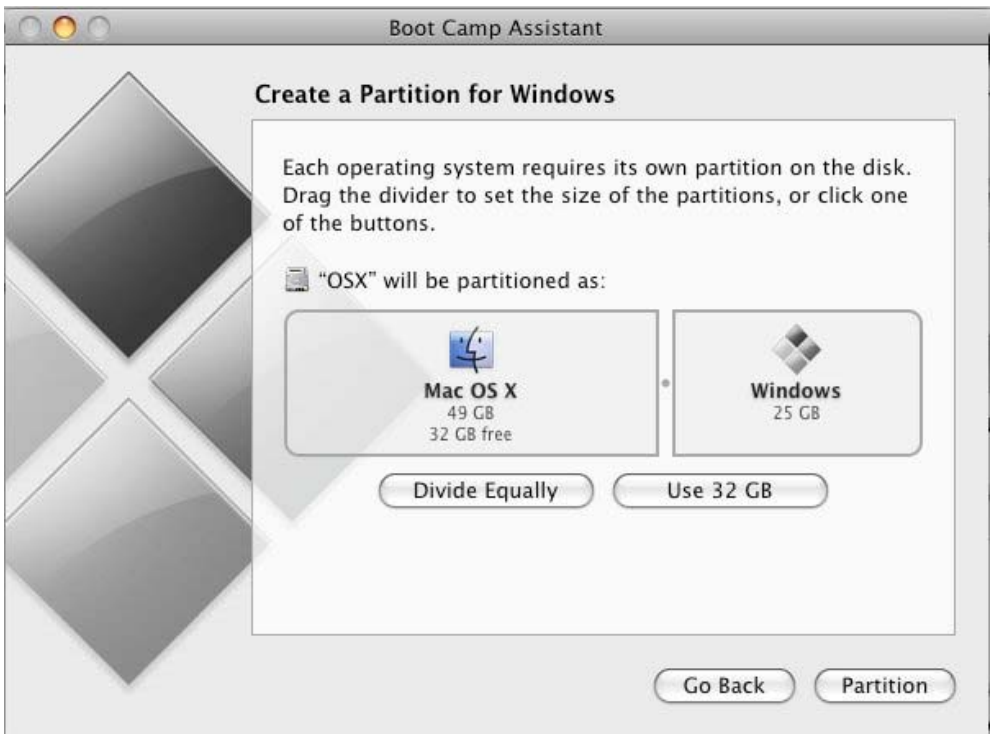
Για να ανακτήσουμε το αντίγραφο ασφαλείας :

1. Αποκτούμε πρόσβαση στην τοποθεσία που βρίσκεται η εικόνα του δίσκου.
2. Προσαρτούμε (mount) την εικόνα του δίσκου και ,αν μας ζητηθεί, βάζουμε τον κωδικό μας για το αρχείο. Αν η εικόνα του δίσκου είναι σε δίκτυο, δεν χρειάζεται να την αντιγράψουμε τοπικά. Θα προσαρτηθεί με ασφάλεια μέσω δικτύου διότι τα δεδομένα είναι με κωδικοποίηση.
3. Αντιγράφουμε τα δεδομένα που θέλουμε στον τοπικό μας υπολογιστή.
4. Αποπροσάρτουμε (Umount) την εικόνα του δίσκου.

Αν έχουμε ρυθμίσει το Time Machine να λειτουργεί σε δίκτυο, τότε εκείνο κάνει χρήση εικονικών δίσκων για κάθε backup. Η μοιραζόμενη τοποθεσία που έχει τον αποθηκευμένο εικονικό δίσκο είναι ασφαλισμένη με κωδικό από τις ρυθμίσεις του Time Machine. Μόνο ο administrator ή έμπιστοι χρήστες θα πρέπει να γνωρίζουν τον κωδικό για όλα τα αντίγραφα ασφαλείας του Time Machine στο δίκτυο.

4.7. Boot Camp

Με την εφαρμογή Boot Camp μπορείτε να εγκαταστήσετε και να τρέξετε άλλα λειτουργικά συστήματα, όπως Windows XP ή Vista στον Intel Mac υπολογιστή σας.



Εικόνα 87 - Παράθυρο Επιλογών Boot Camp

Η εφαρμογή Boot Camp Assistant σας βοηθά να δημιουργήσετε μία κατάτμηση στον σκληρό δίσκο του υπολογιστή σας και στην συνέχεια να εκκινήσετε την εγκατάσταση των Windows.

Όταν κάνετε εγκατάσταση του δευτερευόντως λειτουργικού συστήματος στον intel-based Mac σας, οι λίστες πρόσβασής που έχετε δημιουργήσει με το OS X παύουν να ισχύουν. Με άλλα λόγια, είστε ευάλωτοι σε όλες τις εγγενείς αδυναμίες τοπικής και δικτυακής ασφάλειας που μπορεί να έχει το εναλλακτικό λειτουργικό σύστημα που έχει εγκατασταθεί.

Αν αποφασίσετε τελικά να εγκαταστήσετε ένα δεύτερο λειτουργικό σύστημα, τότε μπορείτε να χρησιμοποιήσετε κωδικοποιημένους εικονικούς δίσκους για να αποθηκεύσετε τα δεδομένα σας όταν χρησιμοποιείτε το OS X. Αυτό προστατεύει τα ευαίσθητα δεδομένα από το να προσπελάζονται από το εναλλακτικό λειτουργικό σύστημα που εγκαταστήσατε.

Επίσης είναι πάντα καλό να διατηρείτε backup των δεδομένων σας στην περίπτωση που η κατάτμηση του δίσκου όπου είναι εγκατεστημένο το OS X καταστραφεί.

5. Συμπεράσματα

Στην παρούσα εργασία προσπαθήσαμε να κάνουμε μια προσέγγιση στα βασικά πεδία ασφάλειας στον κόσμο της Apple. Όπως κάθε σύγχρονο και ευέλικτο λειτουργικό σύστημα, έτσι και το Mac OS X, αποδεικνύεται ασφαλές και έτοιμο να λειτουργήσει ως καταλύτης στις καθημερινές μας ανάγκες. Ο βασικός τομέας της ασφάλειας που μελετήσαμε εδώ, μας έδειξε τους ισχυρούς δεσμούς του συγκεκριμένου λειτουργικού συστήματος με τον κόσμο του UNIX. Μία πλατφόρμα που είναι πρωτοπόρα στην ασφάλεια δεδομένων και δημιουργημένη πάνω στην ανάγκη πολυδιεργασίας. Όλα τα χαρακτηριστικά που διέπουν τον πυρήνα, το περιβάλλον και τους μηχανισμούς ασφάλειας του UNIX, είναι παρόντα και στο Mac OS X.

Η μελέτη των μηχανισμών ασφάλειας σε επίπεδο προσπέλασης τοπικών αρχείων και δικτύωσης, μας έδειξε τα ισχυρά προτερήματα του λειτουργικού συστήματος της Apple. Εκεί που πρέπει να επικεντρώσουμε την προσοχή μας, είναι στο σύστημα Ownership που έχουν όλα τα αρχεία του συστήματός μας και τα καθιστούν σχεδόν απροσπέλαστα σε ιούς και κακόβουλα προγράμματα. Με αυτό το σχετικά απλό, αλλά αφάνταστα σημαντικό χαρακτηριστικό του UNIX, ο απλός χρήστης ταλαιπωρεί και ταλαιπωρείτε από την καθημερινή ενασχόλησή του με τον υπολογιστή.

Αντίστοιχα και με την δικτύωση, η Apple προσφέρει εργαλεία με σχεδίαση λιτή και λειτουργική, προκειμένου να είναι ελκυστικά προς τον χρήστη. Άλλωστε, το καλύτερο πρόγραμμα προστασίας δικτύου είναι εκείνο που δίνει στον χρήστη την δυνατότητα να επέμβει και να καταλάβει την αναγκαιότητά του.

Τέλος, ασχοληθήκαμε με τα προγράμματα εκείνα που είναι απαραίτητα σε όλα τα συστήματα που θέλουν να ονομάζονται «λειτουργικά». Σε κάθε ένα από αυτά, η Apple έχει φροντίσει να ενσωματώσει προχωρημένες ρυθμίσεις που απαιτεί ένας απαιτητικός χρήστης. Αυτό είναι ενδεικτικό του βαθμού προσήλωσης που επιδεικνύει η Apple και στο τεχνικό τομέα. Άλλωστε ξεκίνησε με άριστες περγαμηνές, έχοντας λαμπρά μυαλά να λειτουργούν στο εργαστήριο της έρευνας και ανάπτυξης.

Καταλήγουμε λοιπόν στο συμπέρασμα ότι ασχοληθήκαμε με ένα άριστο λειτουργικό σύστημα. Τόσο άριστο που έχει ήδη αντικατασταθεί από το Mac OS X 10.6 Snow Leopard. Λειτουργία σε 64 Bit και μικρότερες απαιτήσει σε μνήμη! Πέρα όμως από τα στενά πλαίσια μιας τεχνικής ανάλυσης, αν προσεγγίσουμε λίγο πιο προσεχτικά το 'φαινόμενο' Apple, εκείνο που την κάνει να ξεχωρίζει είναι οι συστηματικοί καταναλωτές της. Το λογότυπο του μήλου έχει φανατικούς υποστηρικτές όπου ύστερα με την αρχική τους ενασχόληση με τα προϊόντα του, είτε είναι Mac Mini, OS X, iPod, iPhone iTunes κλπ., έχουν αναθεωρήσει και αυξήσει τις απαιτήσεις τους από τον κόσμο της τεχνολογίας. Ένας από αυτούς δηλώνω και εγώ…

6. Τελική Βιβλιογραφία

URLs :

SecureMac –
http://www.securemac.com/

MacRecon –
http://macrecon.com/how-to-enhance-mac-security/

Επίσημη σελίδα της Apple για ασφάλεια –
http://developer.apple.com/security/

DD's Ultimate Guide to Mac OS Security –
http://homepage.mac.com/macbuddy/SecurityGuide.html

Andreas Schwarz –
http://andreas-s.net/osx- encrypted-swap.html

PacketStorm –
http://packetstormsecurity.org.pk/UNIX/ penetration/rootkits/osxrk-0.2.1.tbz

Βιβλία

Stephen Barker, William Edge (2008) *Foundations of MAC OS X Leopard Security*. Εκδότης : Springer-Verlag New York Inc

David Pogue (2007) *Mac OS X Leopard: The Missing Manual* Εκδότης : Pogue Press

Rob Griffiths (2008) *Mac OS X Hints, Leopard Edition - Macworld Superguide* Εκδότης : Macworld

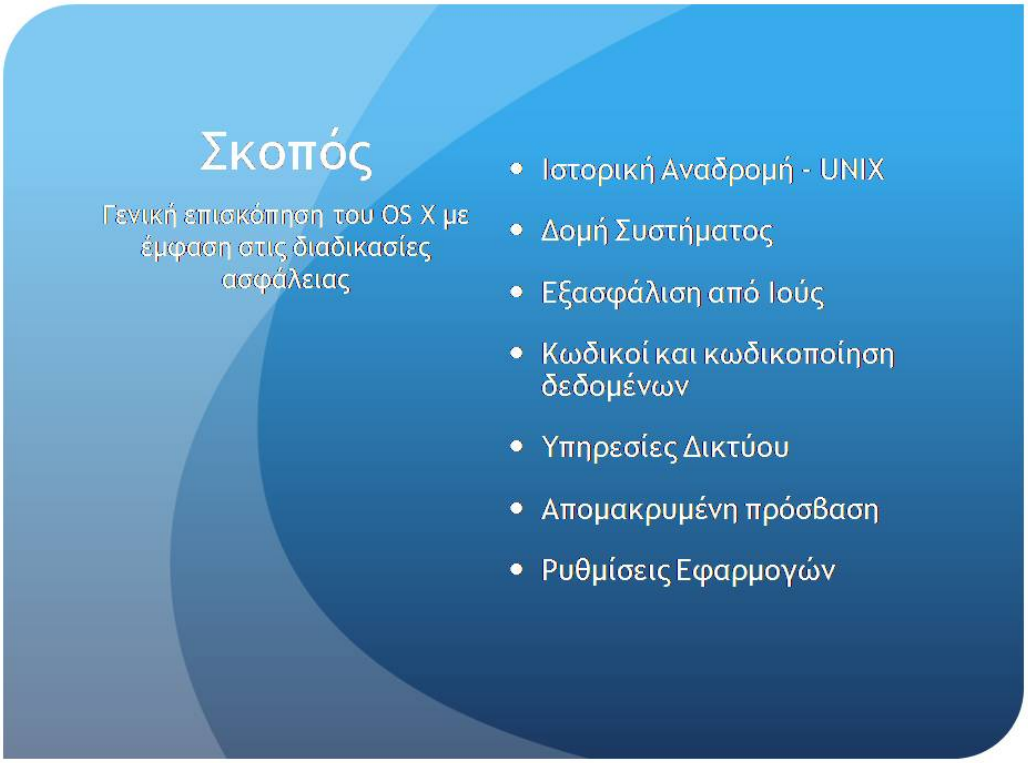
Uthelm Bechtel (2007) *Apple Mac OS X 10.5 Leopard* Εκδότης : Macworld

Apple Inc. (2008) *Mac OS X security configuration for version 10.5 Leopard* Εκδότης : Apple

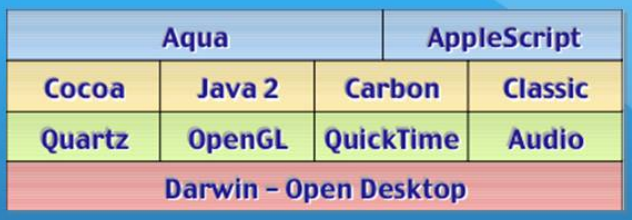
Paul Day (2004) *A guide to security hardening for Apple Mac OS 10.3* Εκδότης : School of Computer Science and Software Engineering at University of Western Australia

Stephen de Vries (2004) *Securing Mac OS X V1.0.doc* Εκδότης : Corsaire Limited

7. Παράρτημα Α



Δομή Συστήματος



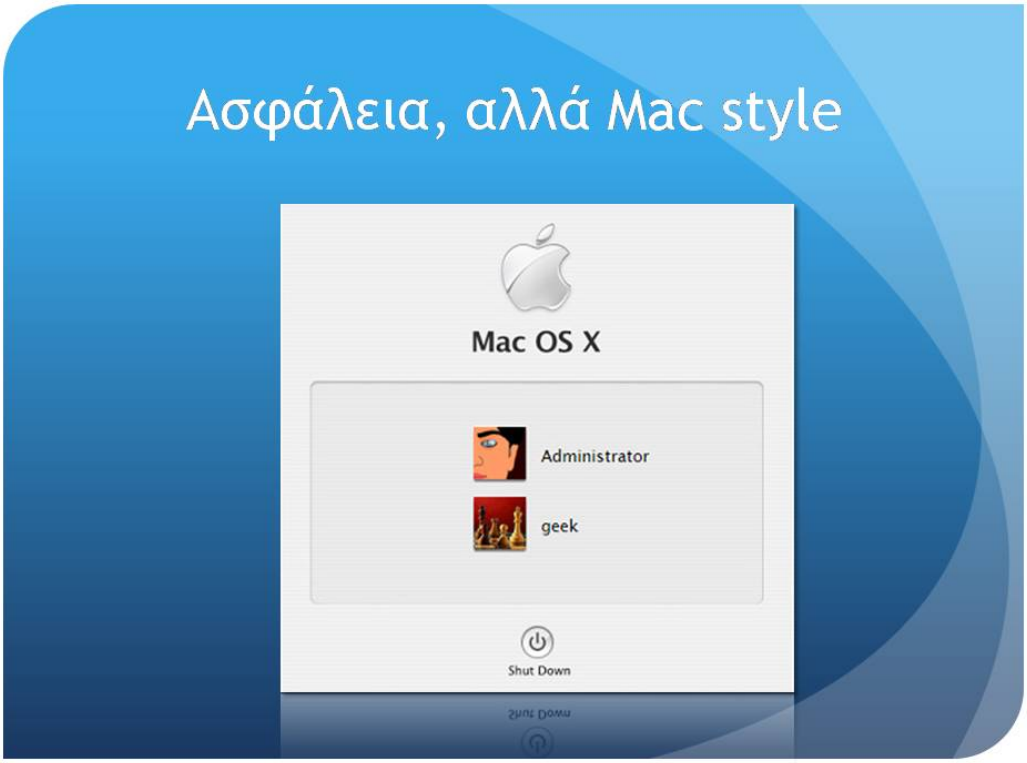
- Προσέγγιση με Layers
- Κόκκινη γραμμή - UNIX
- Πράσινη γραμμή - Σύστημα Γραφικών
- Κίτρινη γραμμή - Σύστημα Υπηρεσιών / Επίπεδο Developer
- Μπλε γραμμή - Σύστημα Διεπαφής / Επίπεδο χρήστη

Εν αρχή... Το UNIX

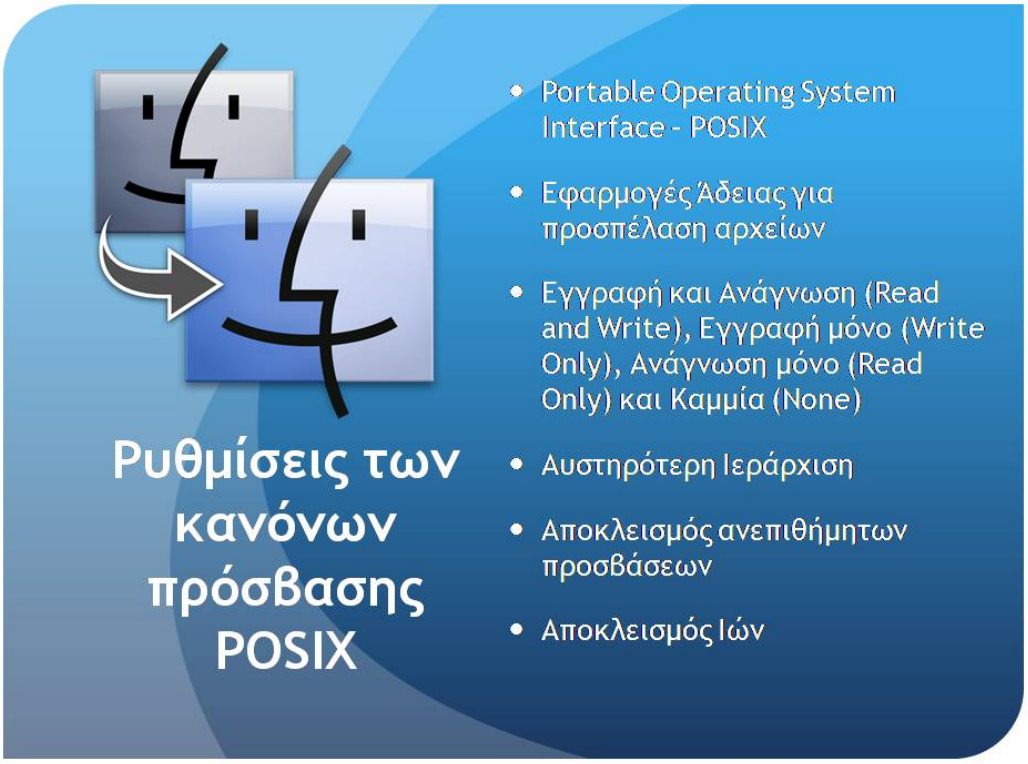
- Κατασκευασμένο με βάση την πολυδιεργασία
- Με ενσωματομένες υπηρεσίες δικτύωσης (εν έτη 1973...)
- Με περιορισμούς πρόσβασης ανά τοπικό και δικτυακό χρήστη
- Με UID και GID (πιστοποιητικά για χρήστες και ομάδες χρηστών)
- Με πυρήνα Open Source, άρα και με συνεχή εξέλιξη


...και εγένετω Apple OS X.
Mac


...και εγένετω Apple OS X.
• Μάρτιος 2001
• Πυρήνας FreeBSD
• Παιδί της NextStep -> Steve Jobs
• Aqua Interface
• Η Dell είχε προτείνει στην Apple να δηλώσει πτώχευση...
• Μετά από την παρουσίαση του OS X, η μετοχή της Apple είχε μεγαλύτερη αξία από την αντίστοιχη της Dell .
• Ανεξάρτητο από CPU brands. Ξεκίνησε από PowerPC, συνέχισε σε x86 και τώρα σε κινητά.
• Και επιτέλους, χωρίς ιούς...


Ασφάλεια, αλλά Mac style
Mac OS X
Administrator
geek
Shut Down


Τοπική ασφάλεια
Αναφορά στην εξασφάλιση των δεδομένων μας σε επίπεδο φυσικής πρόσβασης, δίχως να παρεμβάλεται δικτύωση.
SUPPORT YOUR LOCAL
SECURITY GUARD
• Ρυθμίσεις των κανόνων πρόσβασης POSIX
• Keychain
• Patching
• Κωδικοποίησή δεδομένων


Ρυθμίσεις των κανόνων πρόσβασης POSIX
Portable Operating System Interface - POSIX
Εφαρμογές Άδειας για προσπέλαση αρχείων
Εγγραφή και Ανάγνωση (Read and Write), Εγγραφή μόνο (Write Only), Ανάγνωση μόνο (Read Only) και Καμμία (None)
Αυστηρότερη Ιεράρχιση
Αποκλεισμός ανεπιθήμητων προσβάσεων
Αποκλεισμός Ιών


Keychain - Κλειδούχος
Προεπιλεγμένο λογισμικό αποθήκευσης κωδικών
Ενσωματωμένο μέσα στο λειτουργικό
Ασφαλής αποθήκευση στο MobileMe
Δημιουργία Certificates
Απλό και ισχυρό interface

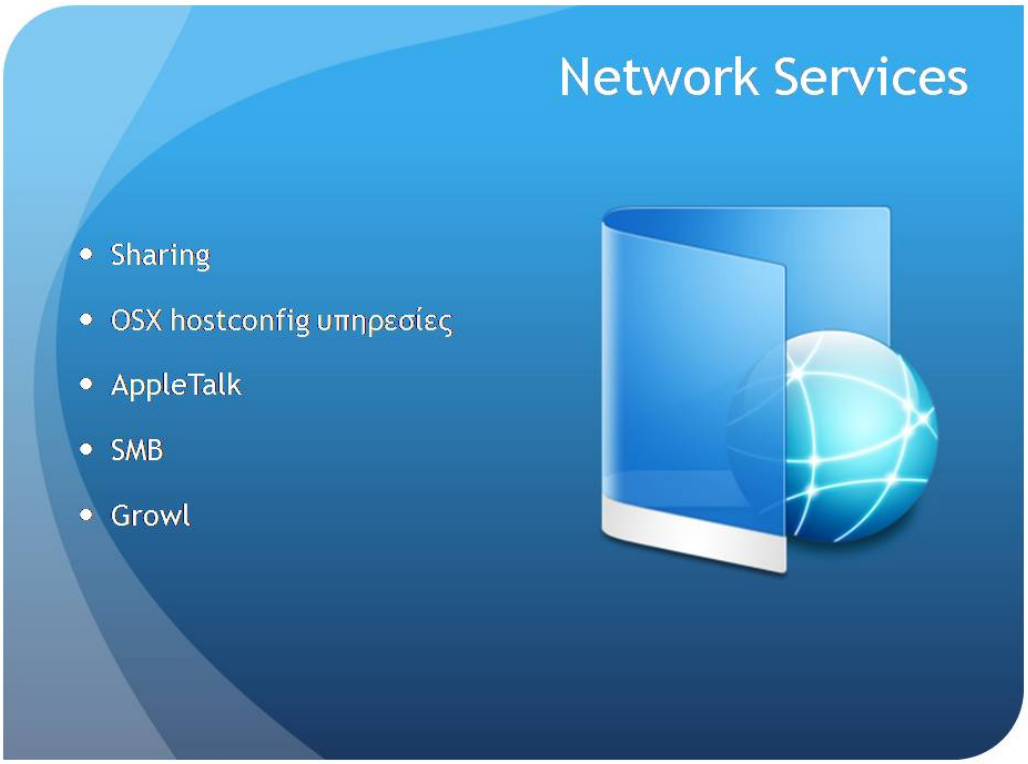
Patching - Updates

- Αυτοματοποιημένο
- Άμεσο προς τον χρήστη
- Απλό και ισχυρό
- Παραμετροποιήσιμο

Κωδικοποίηση δεδομένων

- Χρήση του FileVault
- Προσάρτηση κωδικοποιημένων δίσκων AES
- Συνεχής λειτουργία με μηδενική επίπτωση ταχύτητας
- Ενσωμάτωση GnuPG μέσα στο λειτουργικό
- Κωδικοποίηση ακόμα και του SWAP file!


Δικτυακή Ασφάλεια
Οι μέθοδοι και τεχνικές του OS X για να προστατέψει τα δεδομένα μας σε επίπεδο τοπικού δικτύου, αλλά και Internet.
Network Services
Screen Sharing - VNC
VPN


Network Services
Sharing
OSX hostconfig υπηρεσίες
AppleTalk
SMB
Growl

Screen Sharing - VNC

- Απομακρυσμένη πρόσβαση
- Εμπεριέχει μεγάλα κενά ασφάλειας
- Πρέπει να είμαστε προσεκτικοί στη χρήση του

Ασφάλεια με την χρήση VPN

- Ασφαλίζουμε την απομακρυσμένη επικοινωνία
- VPN Security (L2TP και PPTP)
- L2TP over IPSec
- IPSec

Ασφάλεια στις κυριότερες εφαρμογές

Επισκόπηση για τα μέτρα που μπορούμε να λάβουμε, προκειμένου να ασφαλίσουμε περαιτέρω τις βασικές εφαρμογές του OS X

- iChat
- iTunes
- Apple Firewall
- Safari
- Time Machine
- Boot Camp

- Ενεργοποιούμε το secure chat όπου είναι διαθέσιμο
- Χρησιμοποιούμε την υπηρεσία με χρήστες που γνωρίζουμε
- Την απενεργοποιούμε όπου είναι δυνατόν

iChat

Το εξελιγμένο chat client της Apple


Βάζουμε κωδικό στην βιβλιοθήκη μας
Απενεργοποιούμε τον διαμοιρασμό
Ελέγχουμε τακτικά τον λογαριασμό μας στο online store (αν έχουμε)
iTunes
Η πολυμεσική βιβλιοθήκη

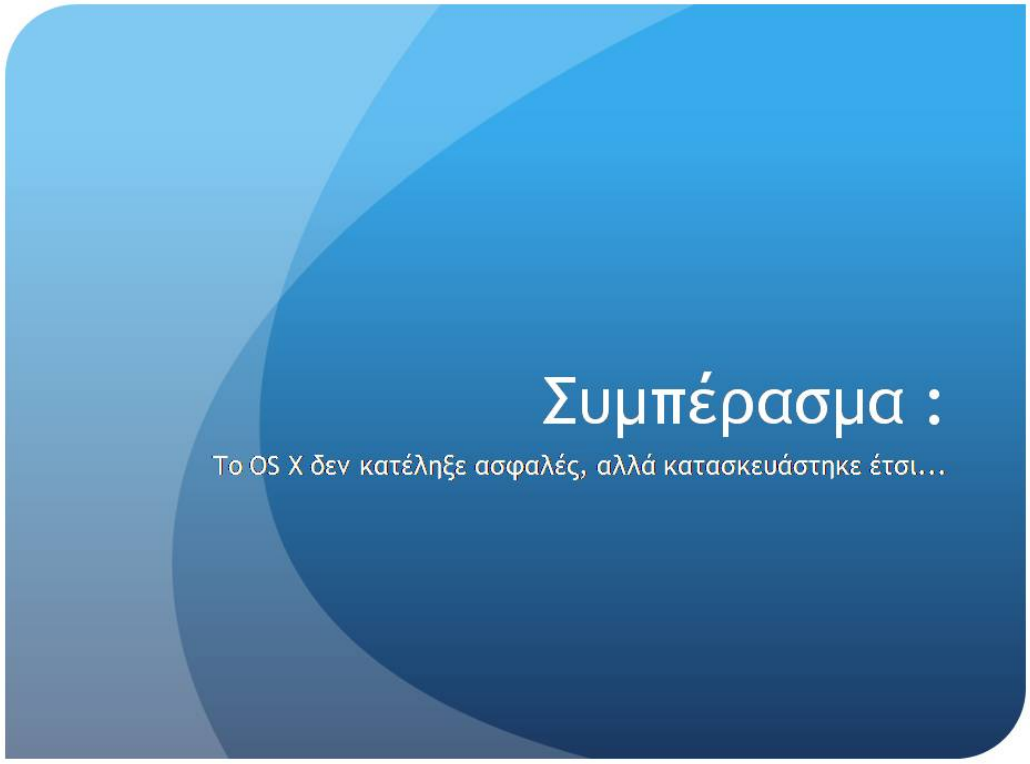

Το ενεργοποιούμε!
Ελέγχουμε τις υπηρεσίες που μας ενδιαφέρουν
Τσεκάρουμε τα κατάλληλα ports
Ενεργοποιούμε το Stealth Mode
Apple Firewall
Το προεγκατεστημένο τοίχος προστασίας


Ενεργοποιούμε το Account Security
Χρησιμοποιούμε ασφαλή σύνδεση με τον Server
Υπογράφουμε ψηφιακά και κωδικοποιούμε τα μηνύματα
Apple Mail
Ο Διαχειριστής Αλληλογραφίας


Απενεργοποιούμε το αυτόματο άνοιγμα
Απενεργοποιούμε τα cookies
Χρησιμοποιούμε την ιδιωτική πλοήγηση πάντα
Safari
Web Browser


Κρατάμε αντίγραφα σε ασφαλή τοποθεσία
Ελέγχουμε την ακεραιότητα του δίσκου
Αν θέλουμε να διαγράψουμε, κάνουμε secure delete
Time Machine
Αντίγραφα ασφαλείας παντού και πάντα


Κάνουμε Backup των δεδομένων μας
Αναγνωρίζουμε ότι εγκαθιστούμε Windows
Κάνουμε το σταυρό μας
Boot Camp
Γιατί τα Mac είναι τα καλύτερα PC


Συμπέρασμα :
Το OS X δεν κατέληξε ασφαλές, αλλά κατασκευάστηκε έτσι...


Ευχαριστώ Πολύ!