Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

Πτυχιακή εργασία

Προστασία δεδομένων σε προσωπικούς υπολογιστές

Μουντοκαλάκης Μιχάλης (ΑΜ: 670)

E-mail: mountokalakis@gmail.com

Επιβλέπων Καθηγητής: Κωνσταντίνος Φυσσαράκης

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 τον καθηγητή, κύριο Κωνσταντίνο Φυσσαράκη που μου εμπιστεύτηκε το συγκεκριμένο θέμα, για την υποστήριξη του καθ ‘όλη την διάρκεια διεκπεραίωσης της παρούσας πτυχιακής.

Επιπλέον, θα ήθελα να ευχαριστήσω την φίλη μου Μαρία Δραμουντανή για την γραμματειακή υποστήριξη και την βοήθεια που μου παρείχε.

Τέλος, ευχαριστώ από καρδίας, την οικογένεια μου, την μητέρα μου Ευαγγελία και τον αδερφό μου Μάνθο, για την συνεχή συμπαράσταση, την αγάπη και την κατανόηση που έδειξαν καθ ‘όλη την διάρκεια των σπουδών μου.

Abstract

The need for security when even using personal computers has gradually increased over the years. The amount of private and sensitive information that are nowadays stored and transferred through personal computers (such as data that include economic and/or personal information etc.) make system security very important. There is a variety of security tools and devices available that protect computers at different levels of security, from which a user can choose. The security combination chosen should take account security strength, usability and cost.

This study, will overview the most popular system security methods, as well as security software and hardware, while taking in account any security weaknesses they may have. In addition, the most important levels of security will be analyzed and explain and a number of different security combinations will be possible, covering different user needs. Lastly full disk encryption software will be presented while in usage and a full security analysis will be made for that software.

Σύνοψη

Στη σύγχρονη εποχή ακόμα και οι οικιακοί χρήστες διαθέτουν στον προσωπικό τους υπολογιστή πληροφορίες και δεδομένα, η εμπιστευτικότητα των οποίων θεωρείται ιδιαίτερα σημαντική (στοιχεία οικονομικής φύσεως, πληροφορίες που αγγίζουν ευαίσθητα προσωπικά δεδομένα κ.α.). Για την προστασία των προαναφερθέντων, υπάρχει μία μεγάλη γκάμα εργαλείων και μεθόδων από τα οποία καλείται ο μέσος χρήστης να επιλέξει (hard disk encryption, tokens κ.α.). Η επιλογή αυτών πρέπει, κατά το δυνατό, να συνδυάζει την ασφάλεια με την ευχρηστία.

Στην παρούσα πτυχιακή θα γίνει επισκόπηση των δημοφιλέστερων μεθόδων, αλλά και εφαρμογών λογισμικού και υλικού που μπορούν να χρησιμοποιηθούν για την προστασία δεδομένων σε Προσωπικούς Υπολογιστές. Θα γίνει συσχέτιση του βαθμού ασφαλείας που ο χρήστης θέλει να επιτύχει (που είναι ανάλογη με την ευαισθησία των δεδομένων), με το κόστος, την ευχρηστία, και την απόδοση του συστήματος. Θα γίνει πειραματική επίδειξη της λειτουργίας ανάλογων εφαρμογών, με διάφορες κλίμακες προσφερόμενης ασφάλειας.

Πίνακας Περιεχομένων

Πίνακας Εικόνων

Πίνακας Screenshot

Κεφάλαιο 1: Εισαγωγή

1.1 Περίληψη

Στη σύγχρονη εποχή ακόμα και οι οικιακοί χρήστες διαθέτουν στον προσωπικό τους υπολογιστή πληροφορίες και δεδομένα η εμπιστευτικότητα των οποίων, θεωρείται ιδιαίτερα σημαντική. Τέτοιες πληροφορίες μπορεί να είναι ευαίσθητα προσωπικά δεδομένα, στοιχεία οικονομικής φύσεως, λογαριασμοί (accounts) διαφόρων χρήσεων, με τους συνοδευτικούς κωδικούς, και γενικά οποιαδήποτε δεδομένα θεωρεί ο ίδιος ο χρήστης κρίσιμα και βρίσκονται αποθηκευμένα στον υπολογιστή του. Για την προστασία των προαναφερθέντων, υπάρχει μία μεγάλη γκάμα εργαλείων και μεθόδων από τα οποία καλείται ο μέσος χρήστης να επιλέξει συνδυάζοντας, κατά το δυνατό, την ασφάλεια με την ευχρηστία.

Στην παρούσα πτυχιακή θα γίνει επισκόπηση των δημοφιλέστερων μεθόδων, και εφαρμογών λογισμικού και υλικού προστασίας δεδομένων, με σκοπό την παρουσίαση και ανάλυση των σημαντικότερων επιπέδων ασφαλείας, ο συνδυασμός των οποίων προσφέρει υψηλή προστασία σε προσωπικούς υπολογιστές (PC), δηλαδή κοινούς (μη εξειδικευμένους) υπολογιστές προσωπικής χρήσης. Η μελέτη αυτή θα εμβαθύνει σε διάφορους τομείς της ασφάλειας υπολογιστών με βάση ένα λειτουργικό σύστημα. Εμείς επιλέγουμε τα Windows καθώς θεωρούνται ως το δημοφιλέστερο λειτουργικό σύστημα και διαθέτουν το μεγαλύτερο εύρος εφαρμογών, οι οποίες είναι κατά κανόνα συμβατές και με παλιότερες εκδόσεις τους. Παίρνουμε ως παραδοχή λοιπόν ότι το λειτουργικό μας σύστημα είναι Windows και θέτουμε τους παρακάτω στόχους.

1.2 Στόχοι

1. Να παρουσιάσουμε και εξηγήσουμε την προστασία που προσφέρει από μόνο του το λειτουργικό σύστημα των Windows και να δείξουμε απλούς τρόπους με τους οποίους ο μέσος χρήστης μπορεί να προστατεύσει τον υπολογιστή του από κοινές απειλές.
2. Να παρουσιάσουμε και εξηγήσουμε τις βασικές μεθόδους κρυπτογράφησης δεδομένων και να εφαρμόσουμε μία από αυτές.
3. Να εξηγήσουμε τα είδη και την χρησιμότητα των συσκευών ασφαλείας για προσωπικούς υπολογιστές και να παρουσιάσουμε μερικές από αυτές.
4. Να αναλύσουμε την έννοια της πλήρους κρυπτογράφησης σκληρού δίσκου, να δούμε με ποιούς τρόπους υλοποιείται και να γνωρίσουμε τις νέες τεχνολογίες σε αυτόν τον τομέα.
5. Τέλος να εφαρμόσουμε πρακτικά ένα παράδειγμα πλήρους κρυπτογράφησης σκληρού δίσκου, να το αναλύσουμε και να παρουσιάσουμε μερικές αδυναμίες του.

1.3 Δομή Εργασίας

Στο κεφάλαιο 2 “Θωράκιση λειτουργικού συστήματος”: θα μελετήσουμε τα συστήματα ασφαλείας ενσωματωμένα στο Windows OS και θα δώσουμε μερικές συμβουλές για να διατηρούμε το σύστημά μας ασφαλές.

Στο κεφάλαιο 3 “Κρυπτογράφηση”: θα εξηγήσουμε την έννοια της κρυπτογράφησης, θα μελετήσουμε τις βασικές μεθόδους κρυπτογράφησης δεδομένων και θα εφαρμόσουμε μία από αυτές.

Στο κεφάλαιο 4 “Συσκευές ασφαλείας”: θα μελετήσουμε τη χρήση και τη λειτουργία των συσκευών ασφαλείας και θα παρουσιάσουμε μερικές από αυτές.

Στο κεφάλαιο 5 “Πλήρης κρυπτογράφηση δίσκου”: θα εξηγήσουμε την έννοια της κρυπτογράφησης δίσκου, θα αναλύσουμε τις τεχνικές υλοποίησης πλήρους κρυπτογράφησης δίσκου και τις νέες τεχνολογίες σε αυτόν τον τομέα.

Στο κεφάλαιο 6 “Εφαρμογή πλήρους κρυπτογράφησης δίσκου”: θα εφαρμόσουμε πρακτικά πλήρη κρυπτογράφηση δίσκου παρουσιάζοντας και εξηγώντας την διαδικασία βήμα βήμα. Τέλος θα παρουσιάσουμε μερικές αδυναμίες της εφαρμογής και θα καταλήξουμε σε κάποια συμπεράσματα και προτάσεις.

1.4 Σχεδιάγραμμα

Αριθμός κεφαλαίου	Τίτλος
1	Εισαγωγή
2	Θωράκιση λειτουργικού συστήματος
3	Κρυπτογράφηση
4	Συσκευές ασφαλείας
5	Πλήρης κρυπτογράφηση δίσκου
6	Εφαρμογή πλήρους κρυπτογράφησης δίσκου

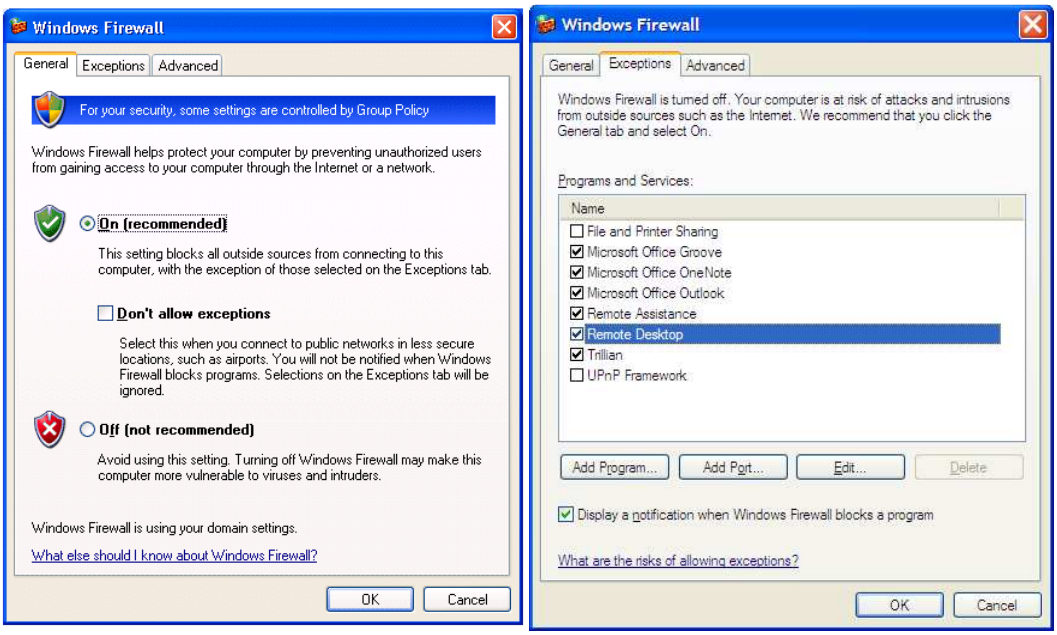
Κεφάλαιο 2: Θωράκιση λειτουργικού συστήματος

2.1 Συστήματα ασφάλειας ενσωματωμένα στο λειτουργικό σύστημα

Η ραγδαία ανάπτυξη και εξάπλωση των υπολογιστικών συστημάτων και του διαδικτύου είχαν ως φυσικό επακόλουθο, την αντίστοιχη ανάπτυξη στη δημιουργία και διάδοση κακόβουλου λογισμικού. Οι απειλές αυτές, σε συνδυασμό με την ποικιλία τους αλλά και την ευκολία που μπορεί να τις συναντήσει οποιοσδήποτε χρήστης, ανάγκασε τις μεγάλες εταιρίες παραγωγής λειτουργικών συστημάτων να ενσωματώσουν σταδιακά στα λειτουργικά τους συστήματα, κάποια βασικά συστήματα ασφάλειας. Παρακάτω θα παρουσιάσουμε και θα αναλύσουμε τα πιο σημαντικά από αυτά τα συστήματα που έχουν ενσωματωθεί κατά καιρούς στις διάφορες ανανεώσεις του λειτουργικού συστήματος Windows της Microsoft (1).

2.1.1 Windows Firewall

Πιο συγκεκριμένα, η Microsoft στην έκδοση του λειτουργικού συστήματος Windows XP μεταξύ των πολλών βελτιώσεων ασφάλειας και προστασίας ιδιωτικών δεδομένων ενσωμάτωσε για πρώτη φορά ένα software firewall, δηλαδή ένα τείχος προστασίας σε επίπεδο λογισμικού που ονόμασε ICF. Στις μετέπειτα εκδόσεις Windows αναφέρεται απλά ως Windows Firewall (2) (Εικόνα 1.α) και ουσιαστικά είναι ένα φίλτρο που ελέγχει τα πακέτα που διακινούνται στο δίκτυο με βάση τις πληροφορίες κεφαλής που έχει κάθε πακέτο (IP πηγής, IP προορισμού, port) και τους κανόνες που έχουν τεθεί έχοντας τη δυνατότητα να δέχεται ή να αρνείται την κίνηση. Με αυτό τον τρόπο αποκλείει δεδομένα που προέρχονται από οποιαδήποτε αυθαίρετη και πιθανώς επικίνδυνη πηγή. Ο χρήστης, μέσω ενός απλού μενού, μπορεί να ανοίγει και κλείνει όποια ports επιθυμεί και να εξουσιοδοτεί εφαρμογές (Εικόνα 1.β).

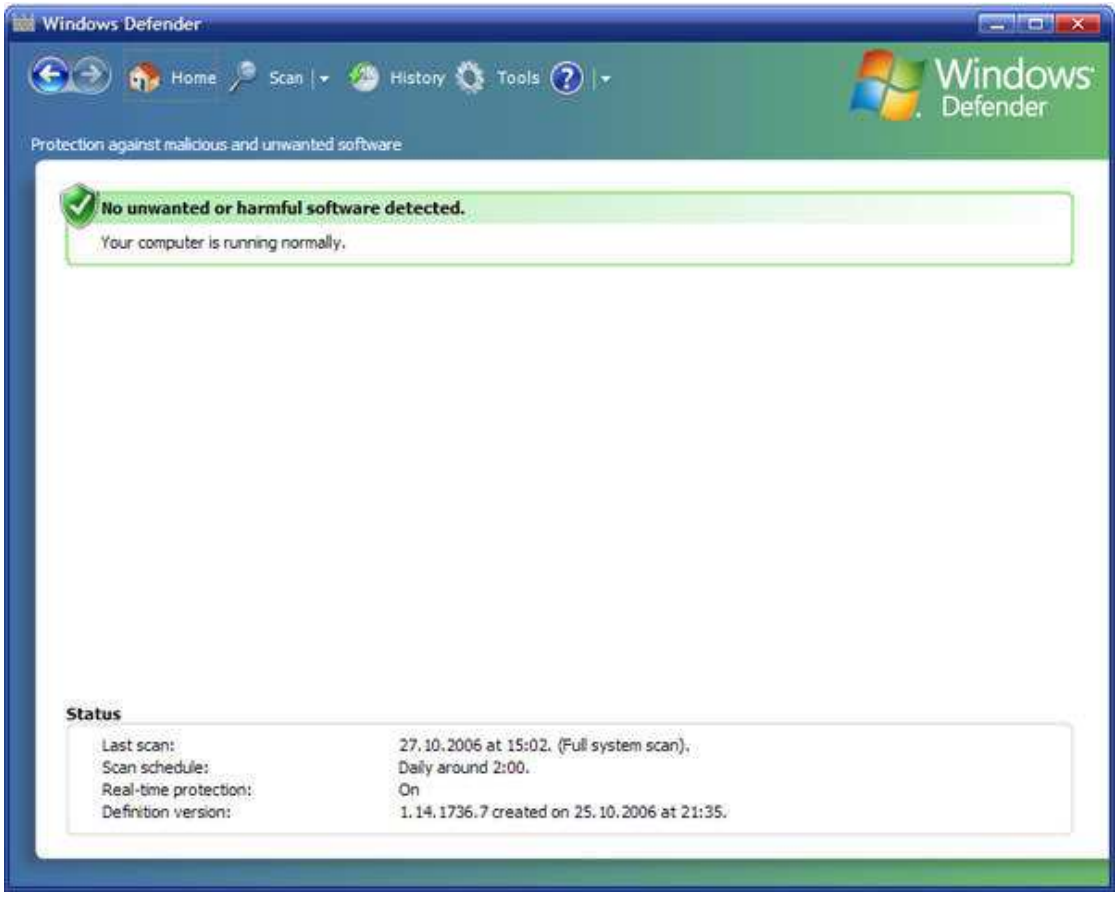


Εικόνα 1 α) Windows Firewall **β) Μενού διαχείρισης προγραμμάτων και port**

2.1.2 Windows Defender

Στην επόμενη έκδοση του λειτουργικού συστήματος από την Microsoft, τα Windows Vista, προστέθηκε ο Windows Defender (3) (Εικόνα 2), ένα πρόγραμμα καταπολέμησης spyware (λογισμικό κατασκόπευσης) και άλλου παρόμοιου κακόβουλου λογισμικού. Τα κύρια χαρακτηριστικά του είναι τα εξής:

1. Προστασία και έλεγχος σε πραγματικό χρόνο
2. Σύνδεση με την κοινότητα του SpyNet που δίνει πληροφορίες για πιστοποιημένα από την κοινότητα προγράμματα.
3. Δυνατότητα πλήρους σάρωσης του pc για κακόβουλο λογισμικό και προγραμματισμού για επαναλαμβανόμενες σαρώσεις ανά τακτά χρονικά διαστήματα.



Εικόνα 2 Windows Defender

2.1.3 Λοιπά ενσωματωμένα συστήματα

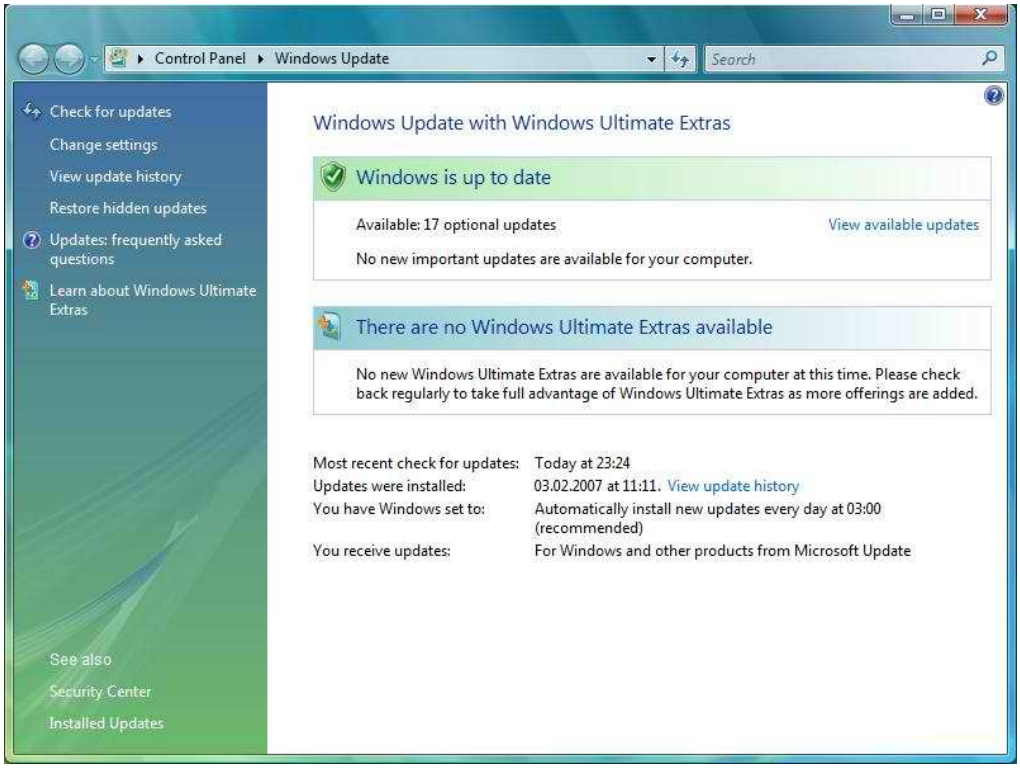
Τα Windows σε κάθε νέα έκδοση βελτιώνουν το υπάρχον λογισμικό προστασίας προσθέτοντας συνήθως και νέα μέτρα ασφάλειας. Παρακάτω θα αναφέρουμε μερικά από αυτά θεωρώντας πλέον ότι διαθέτουμε Windows 7, την πιο πρόσφατη έκδοση λειτουργικού συστήματος της Microsoft.

1) Έλεγχος λογαριασμού χρήστη (UAC): Εμποδίζει μη εξουσιοδοτημένες αλλαγές στον υπολογιστή. Ουσιαστικά δηλαδή περιορίζει τα δικαιώματα όλων των εφαρμογών, ώστε να απαιτείται η εξουσιοδότηση τους από το χρήστη για να πραγματοποιήσουν οποιαδήποτε ενέργεια.
2) Κέντρο ασφαλείας των Windows: Εμφανίζει σημαντικές πληροφορίες για την κατάσταση ασφάλειας του pc, ελέγχοντας διάφορα στοιχεία και ρυθμίσεις ασφαλείας συμπεριλαμβανομένων των συστημάτων που έχουμε προαναφέρει και όχι μόνο.
3) Κέντρο αντιγράφων ασφαλείας και επαναφοράς των Windows: Δίνει στον χρήστη τη δυνατότητα να δημιουργεί αντίγραφα ασφαλείας οποιουδήποτε αρχείου αλλά και ολόκληρου του συστήματος. Σε περίπτωση μη αναστρέψιμης καταστροφής στο λογισμικό των Windows ο χρήστης μπορεί να επαναφέρει τον υπολογιστή του στην κατάσταση που ήταν όταν δημιουργήθηκε το αντίγραφο ασφαλείας.
4) Τέλος κάποιες εκδόσεις των Windows 7 όπως η Business και η Ultimate προσφέρουν μια επιπλέον δυνατότητα ασφαλείας που ονομάζεται κρυπτογράφηση μονάδων δίσκου BitLocker και παρέχει άλλο ένα επίπεδο προστασίας κρυπτογραφώντας όλα τα δεδομένα που είναι αποθηκευμένα στον τόμο του λειτουργικού συστήματος των Windows. Στο κεφάλαιο 5 θα εξηγήσουμε αναλυτικότερα πως λειτουργεί το BitLocker και γενικά κάθε τέτοιου είδους λογισμικό.

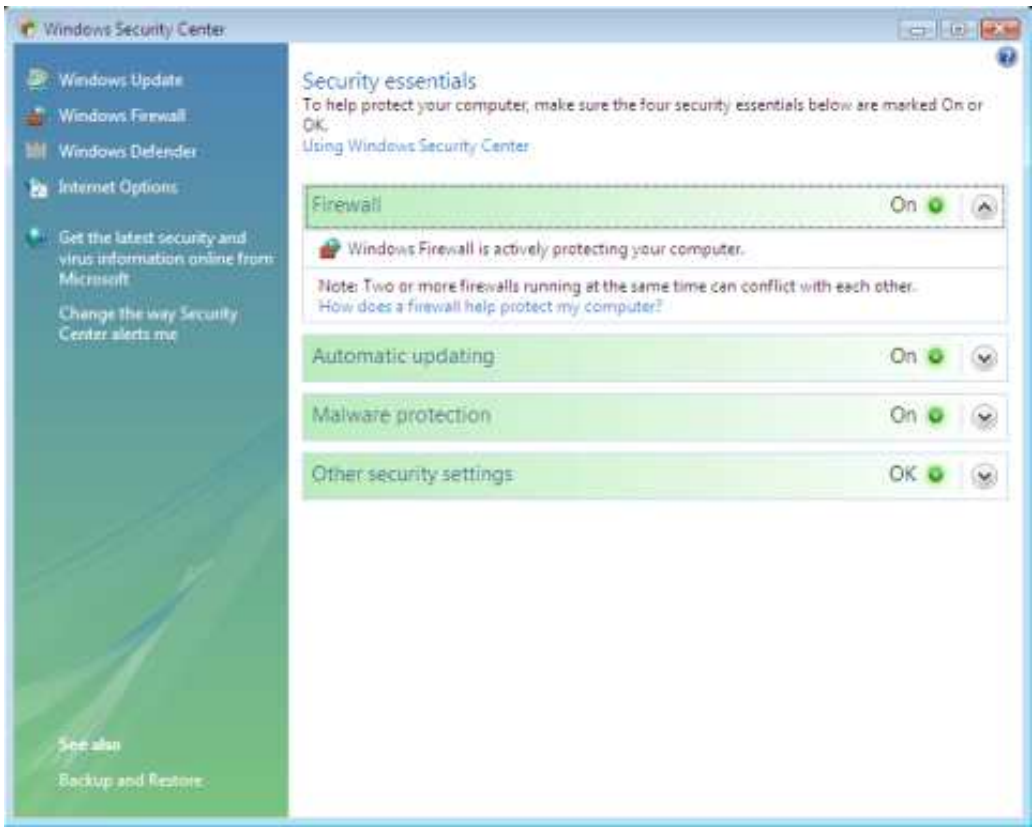
2.2 Συντήρηση λειτουργικού συστήματος

Όπως προαναφέραμε η εξέλιξη του κακόβουλου λογισμικού και η ανακάλυψη κενών ασφαλείας στα λειτουργικά συστήματα δημιουργούν την ανάγκη συνεχούς αναβάθμισης του λειτουργικού συστήματος και όλων των υποσυστημάτων ασφαλείας που βρίσκονται ενσωματωμένα σε αυτό. Για τον λόγο αυτό υπάρχει το Windows Update (Εικόνα 3), το οποίο αναλαμβάνει να ενημερώνει οποιοδήποτε μέρος του συστήματος χρειάζεται αναβάθμιση.

Επιπλέον το Κέντρο Ασφάλειας (Εικόνα 4) που προαναφέραμε αναλαμβάνει να ειδοποιεί τον χρήστη σε περίπτωση κάποιου προβλήματος ή δυσλειτουργίας στα υποσυστήματα που ελέγχει.



Εικόνα 3 Windows Update



Εικόνα 4 Κέντρο Ασφαλείας Windows

2.3 Επιπλέον προστασία

Για να είναι σε θέση το pc να αντιμετωπίσει οποιαδήποτε (ή σχεδόν οποιαδήποτε) απειλή συναντήσουμε στον συνεχώς μεταβαλλόμενο κόσμο του internet, είναι απαραίτητη η εγκατάσταση επιπλέον λογισμικού. Το βασικότερο από αυτά είναι το λεγόμενο αντιϊκό λογισμικό (antivirus). Όπως αναφέρει και η Βικιπαίδεια (4) «*προκειμένου να εξασφαλίσουν την απρόσκοπτη και χωρίς μολύνσεις λειτουργία ενός συστήματος, τα αντιϊκά εκκινούν ταυτόχρονα με το λειτουργικό σύστημα του υπολογιστή, χωρίς εντολές από το χρήστη, και παραμένουν ως διαδικασίες στη μνήμη ώστε να είναι σε θέση να ανιχνεύουν τυχόν μολύνσεις σε πραγματικό χρόνο.*»

Πολλές εταιρίες αναπτύσσουν αντιϊκές εφαρμογές και υπάρχει πληθώρα επιλογών για τον μέσο χρήστη που μπορεί να βρει οικονομικές λύσεις αλλά ακόμα και δωρεάν αντιϊκό λογισμικό. Ενδεικτικά αναφέρονται οι εταιρίες Norton, Eset, Avast, AVG, από τις οποίες οι δύο τελευταίες είναι μεταξύ των εταιριών που διαθέτουν και δωρεάν έκδοση του λογισμικού τους.

2.4 Απλές μέθοδοι προστασίας συστήματος

Όλα τα παραπάνω δημιουργούν ένα δίχτυ ασφαλείας στο pc. Για να είναι όμως αποτελεσματικό αυτό το δίχτυ πρέπει να δοθεί προσοχή σε ορισμένα κρίσιμα σημεία:

1. Συνεχής και άμεση αναβάθμιση του λειτουργικού συστήματος και των υποσυστημάτων του όταν είναι διαθέσιμες ενημερωμένες εκδόσεις (Το Windows Update να έχει ρυθμιστεί για αυτόματη εγκατάσταση ενημερώσεων).
2. Συνεχής αναβάθμιση του αντιϊκού λογισμικού και ενημέρωση της βάσης δεδομένων αντιμετώπισης ιών (Τα πιο πολλά αντιϊκά προγράμματα κάνουν αυτόματη ενημέρωση αρκεί ο χρήστης να είναι συνδεμένος στο διαδίκτυο).
3. Το Windows Firewall και γενικά όλα τα συστήματα ασφαλείας πρέπει να είναι πάντοτε ενεργοποιημένα ειδικά όταν ο χρήστης είναι συνδεμένος στο διαδίκτυο.
4. Να έχουν οριστεί προγραμματισμένες εργασίες (Scheduled Tasks), δηλαδή εργασίες που ρυθμίζει ο χρήστης και επαναλαμβάνονται ανά τακτά χρονικά διαστήματα από μόνες τους. Ενδεικτικά εφαρμογές που υποστηρίζουν προγραμματισμένες εργασίες είναι το Windows Defender, το κέντρο αντιγράφων ασφαλείας και επαναφοράς των Windows, το αντιϊκό λογισμικό αλλά και γενικότερα, οι περισσότερες εφαρμογές ασφαλείας ενδέχεται να έχουν αυτή τη δυνατότητα.

Κεφάλαιο 3: Κρυπτογράφηση

3.1 Βασικές έννοιες

Η έννοια της κρυπτογράφησης όπως αναφέρεται στη Βικιπαίδεια (5) είναι η εξής: «*Κρυπτογράφηση (encryption) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με την χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη. Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση (decryption).*»

Σε γενικές γραμμές, η κρυπτογράφηση και αποκρυπτογράφηση γίνεται με τη χρήση ενός αλγόριθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης. Επειδή ο αλγόριθμος κρυπτογράφησης, δηλαδή η μεθοδολογία με την οποία κρυπτογραφούνται τα δεδομένα μπορεί να είναι γνωστή σε οποιονδήποτε, η εμπιστευτικότητα των κρυπτογραφημένων πληροφοριών βασίζεται στην μυστικότητα του κλειδιού κρυπτογράφησης ή ακόμα και στον συνδυασμό δημόσιου και ιδιωτικού κλειδιού όπως θα δούμε παρακάτω σε κάποιες τεχνικές.

Το μέγεθος αυτών των κλειδιών μετριέται σε αριθμό bits και γενικά ισχύει ο εξής κανόνας: όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί η κρυπτογραφημένη πληροφορία από κάποιον υποκλοπέα. Πρέπει να σημειώσουμε εδώ ότι διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

3.2 Κρυπτογράφηση δεδομένων

Κρυπτογραφώντας πληροφορίες ή δεδομένα που θεωρούνται εμπιστευτικά τους προσδίδουμε ακόμα ένα επίπεδο ασφάλειας. Η κρυπτογράφηση δεδομένων λοιπόν χωρίζεται σε τρείς βασικές κατηγορίες ανάλογα με την τεχνική κρυπτογράφησης που εφαρμόζει:

- Κρυπτογράφηση συμμετρικού κλειδιού
- Κρυπτογράφηση δημοσίου κλειδιού
- Ψηφιακή στεγανογραφία

3.2.1 Κρυπτογράφηση συμμετρικού κλειδιού

Η κρυπτογράφηση συμμετρικού κλειδιού χρησιμοποιεί ένα κοινό κλειδί κατά την διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού αυτού. Μερικοί από τους πιο διαδεδομένους αλγόριθμους κρυπτογράφησης συμμετρικού κλειδιού είναι οι εξής:

- AES
- Blowfish
- CAST
- DES, 3DES
- Serpent
- Twofish

Ο AES (Advanced Encryption Standard) είναι ίσως ο πιο διαδεδομένους συμμετρικός αλγόριθμος και εφαρμόζει κατά την κρυπτογράφηση τρείς διαδοχικούς αλγόριθμους τον AES-128, AES-192 και AES-256. Καθένας από αυτούς ενεργεί σε blocks (περιοχές σταθερού μήκους bit) με μέγεθος 128, 192 και 256 bit αντίστοιχα. Ουσιαστικά χρησιμοποιεί ως «καλούπι» ένα πίνακα 4X4 bytes και επαναλαμβανόμενους γύρους διεργασιών, εφαρμόζοντας τους προαναφερθέντες αλγόριθμους διαδοχικά για να μετατρέψει τα δεδομένα εισόδου σε κρυπτογραφημένα δεδομένα. Κατά την αποκρυπτογράφηση εφαρμόζει ανάποδα τους επαναλαμβανόμενους αυτούς γύρους διεργασιών (6).

Υπάρχουν πάρα πολλά προγράμματα που εφαρμόζουν την κρυπτογράφηση συμμετρικού κλειδιού, ένα από αυτά που μπορεί να χρησιμοποιήσει και να εφαρμόσει τους περισσότερους από τους προαναφερόμενους αλγόριθμους, για εκπαιδευτικό κυρίως σκοπό, είναι το TrueCrypt (7).

3.2.2 Κρυπτογράφηση δημοσίου κλειδιού

Η κρυπτογράφηση δημοσίου κλειδιού ή κρυπτογράφηση ασύμμετρου κλειδιού έχει δυο είδη κλειδιών. Ένα δημόσιο που χρησιμοποιείται για την κρυπτογράφηση, και ένα ιδιωτικό για την αποκρυπτογράφηση. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Το μήνυμα που κρυπτογραφείται με το δημόσιο κλειδί δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με τη χρήση του ιδιωτικού κλειδιού που είναι συνδεμένο με αυτό.

Η πιο διαδεδομένη εφαρμογή κρυπτογράφησης δημοσίου κλειδιού είναι το PGP (8). Αρχικά και όταν δημιουργήθηκε το 1991 προσέφερε ασφαλή επικοινωνία, μεταξύ των χρηστών, σε συστήματα που χρησιμοποιούσαν λογισμικό BBS. Σταδιακά αναπτύχθηκε και επέκτεινε την χρήση του υποστηρίζοντας και άλλες εφαρμογές μεταξύ αυτών και εφαρμογές ηλεκτρονικού ταχυδρομείου. Από το 2010 και μετά συνενώθηκε με την εταιρία παραγωγής αντιϊκού λογισμικού Symantec και πλέον αποτελείται από μια σουίτα λογισμικού με πληθώρα προγραμμάτων που προσφέρουν κρυπτογράφηση, προστασία δεδομένων, αλλά και πλήρη κρυπτογράφηση σκληρού δίσκου. Τέλος υπάρχουν και δωρεάν προγράμματα όπως το GnuPG που υποστηρίζει αρκετά λειτουργικά συστήματα μεταξύ των οποίων και Windows.

3.2.3 Ψηφιακή στεγανογραφία

Η ψηφιακή στεγανογραφία (9) είναι ένα είδος κρυπτογράφησης και χρησιμοποιείται για την απόκρυψη δεδομένων ή/και πληροφοριών μέσα σε άλλα δεδομένα που δεν προδίδουν το περιεχόμενο τους, όπως αρχεία εικόνας, ήχου ή ακόμα και εκτελέσιμα αρχεία (exe). Η πιο διαδεδομένη χρήση της ψηφιακής στενογραφίας είναι η απόκρυψη κειμένου σε εικόνες, το κείμενο συμπιέζεται συνήθως με κωδικοποίηση Huffman (10), κρυπτογραφείται με συμμετρικό κλειδί για περισσότερη ασφάλεια και τέλος ενσωματώνεται στην εικόνα. Ένα δωρεάν πρόγραμμα που επιτρέπει απόκρυψη κειμένου σε αρχεία εικόνων ή ήχου και την αντίστροφη μετατροπή τους είναι το Xiao Steganography (11).

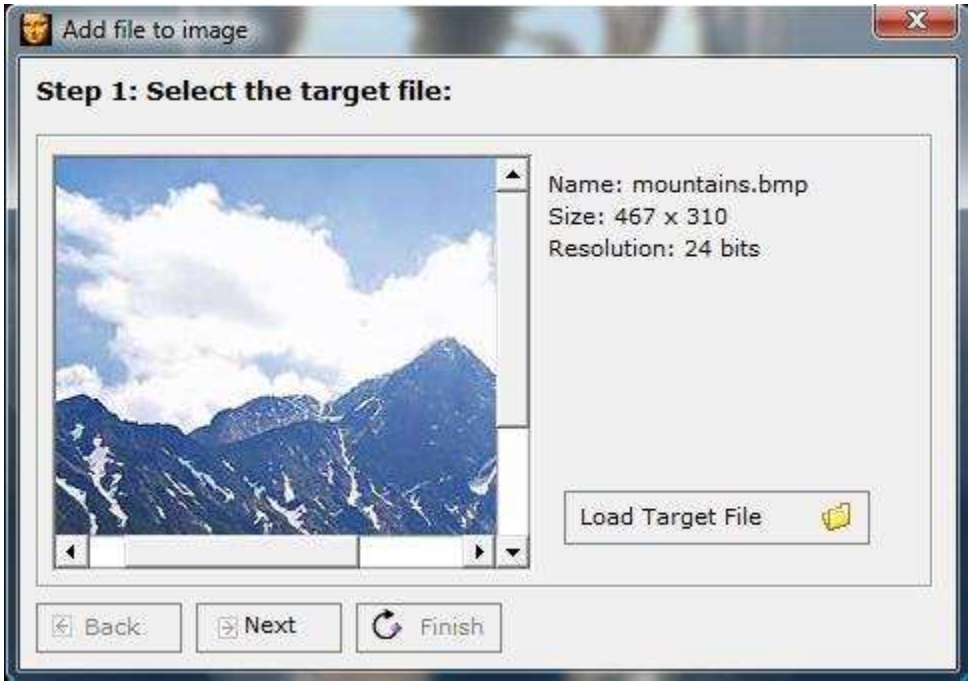
3.3 Απόκρυψη πληροφοριών με Xiao Steganography

Αφού ο χρήστης κατεβάσει και εγκαταστήσει το δωρεάν λογισμικό, Xiao Steganography (11), εκκινεί την εφαρμογή (Screenshot 1).

Για να αποκρύψουμε πληροφορίες σε ένα αρχείο πατάμε το κουμπί “Add Files”.

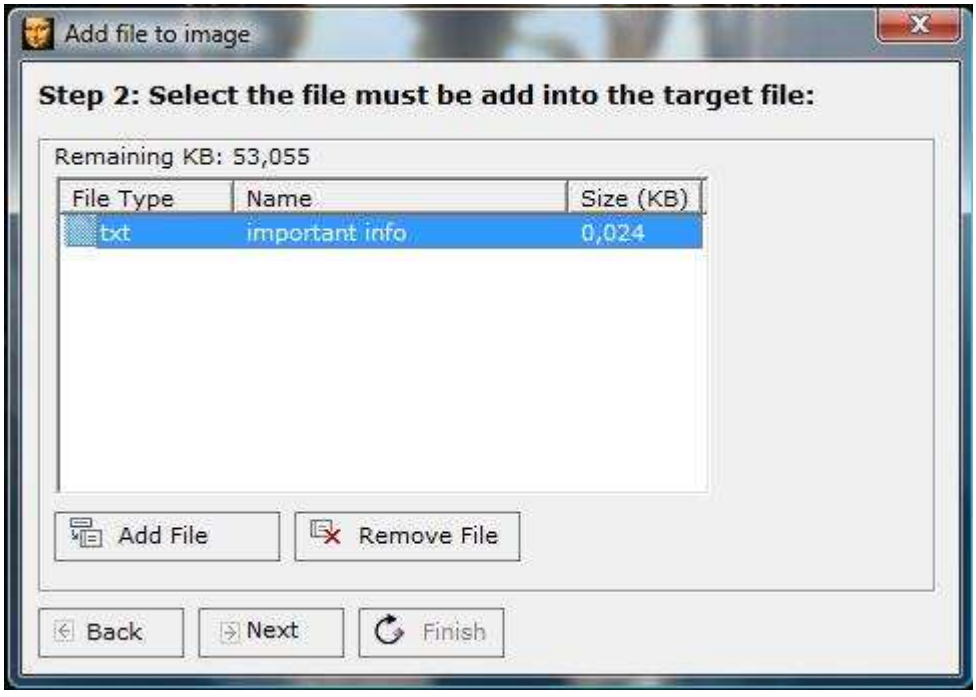
Screenshot 1 Κυρίως Μενού Xiao Steganography

Βήμα 1ο: Στη συνέχεια και πατώντας το κουμπί “Load Target File”, ο χρήστης καλείται να επιλέξει μία εικόνα (.bmp) ή ένα αρχείο ήχου (.wav), μέσα στο οποίο θα αποκρυφτούν πληροφορίες. Σε αυτή την δοκιμή επιλέξαμε την εικόνα mountains.bmp (Screenshot 2).



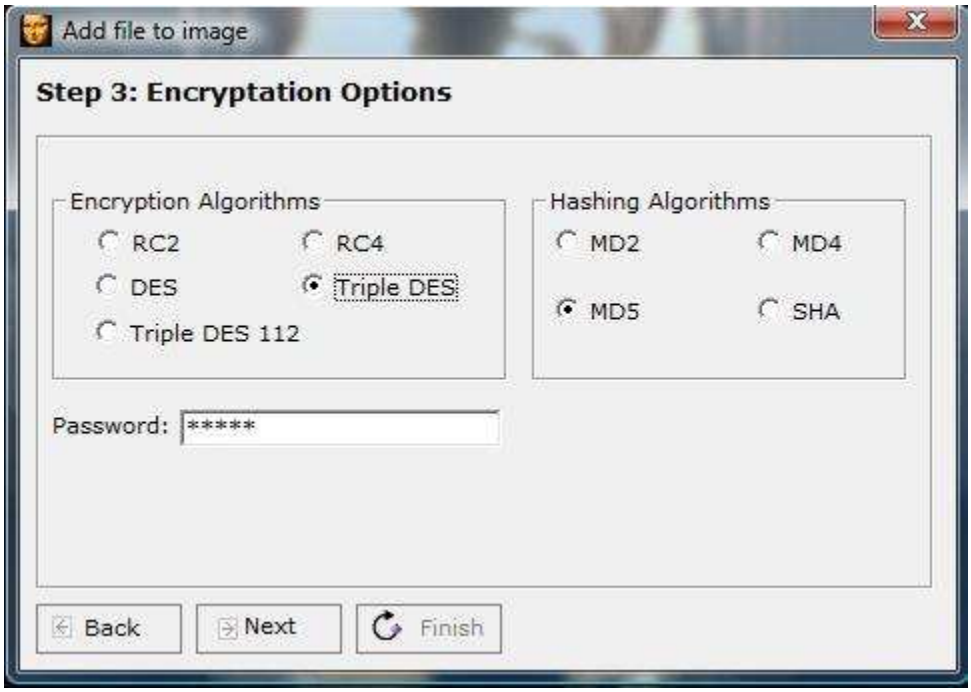
Screenshot 2 Επιλογή αρχείου μέσα στο οποίο θα γίνε απόκρυψη της πληροφορίας

Βήμα 2ο: Στο επόμενο βήμα, ο χρήστης καλείται να επιλέξει ένα ή περισσότερα αρχεία κειμένου (.txt) που περιέχουν τις πληροφορίες προς απόκρυψη και να τα φορτώσει στην εφαρμογή πατώντας το κουμπί “Add File”. Ως επιπλέον πληροφορία, η εφαρμογή εμφανίζει, πόσος χώρος σε KB υπάρχει ελεύθερος (Remaining KB), στο αρχείο που επέλεξε ο χρήστης στο βήμα 1. Κατά συνέπεια το συνολικό μέγεθος των αρχείων που θα αποκρυφτούν δεν μπορεί να ξεπερνάει τον διαθέσιμο ελεύθερο χώρο. Στην περίπτωσή μας φορτώσαμε το αρχείο important info.txt (Screenshot 3).



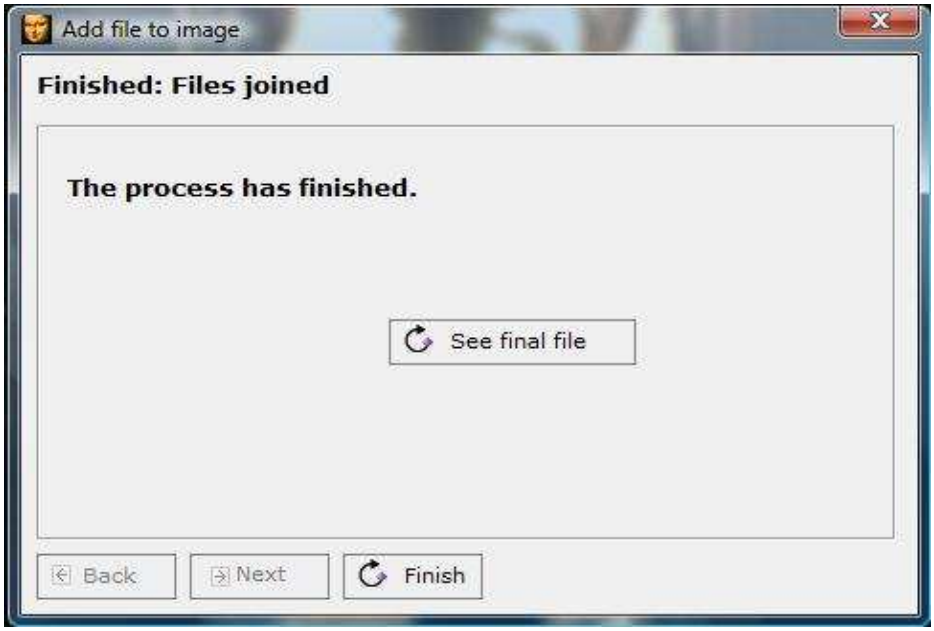
Screenshot 3 Επιλογή αρχείου προς απόκρυψη

Βήμα 3ο: Ο χρήστης καλείται να επιλέξει τον αλγόριθμο κρυπτογράφησης και τον αλγόριθμο κατακερματισμού, που θα χρησιμοποιηθούν για την κρυπτογράφηση των πληροφοριών, καθώς και τον μυστικό κωδικό μέσω του οποίου θα γίνεται η αποκρυπτογράφηση. Εμείς επιλέξαμε 3DES και MD5 αντίστοιχα και θέσαμε ένα 5ψήφιο κωδικό (Screenshot 4).



Screenshot 4 Επιλογή αλγορίθμου κρυπτογράφησης, κατακερματισμού και μυστικού κωδικού

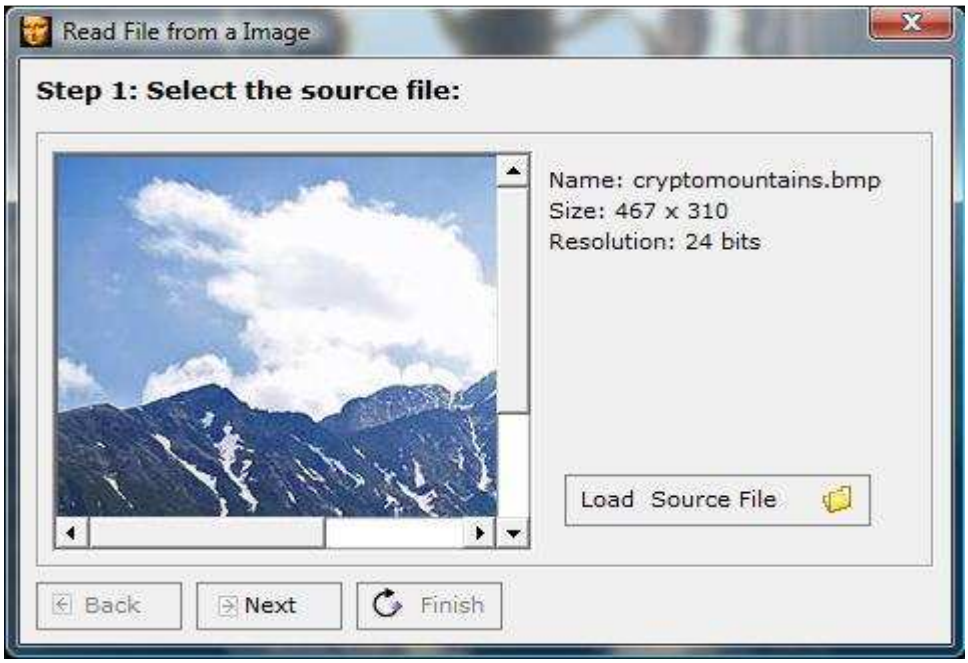
Βήμα 4ο: Τέλος ο χρήστης επιλέγει το όνομα του νέου αρχείου ήχου/εικόνας που θα δημιουργηθεί, το οποίο θα είναι εμφανισιακά ίδιο με το αρχικό, εμπερικλείοντας και τις κρυπτογραφημένες πληροφορίες. Η διαδικασία της απόκρυψης κρυπτογραφημένων πληροφοριών στο αρχείο, ολοκληρώθηκε (Screenshot 5).



Screenshot 5 Ολοκλήρωση της απόκρυψης πληροφοριών στο αρχείο

Αντίστροφα, για να επανακτήσει ο χρήστης πληροφορίες που εμπεριέχονται κρυμμένες σε ένα αρχείο, επιστρέφει στο κυρίως μενού της εφαρμογής και πατάει το κουμπί “Extract File” (Screenshot 1).

Βήμα 1ο: Επιλέγει το αρχείο που περιέχει τις κρυμμένες πληροφορίες και το φορτώνει στην εφαρμογή πατώντας το κουμπί “Load Source File” (Screenshot 6).



Screenshot 6 Επιλογή αρχείου που περιέχει κρυμμένες πληροφορίες

Βήμα 2ο: Η εφαρμογή εμφανίζει τα αρχεία που εμπεριέχονται κρυπτογραφημένα, για να γίνει όμως αποκρυπτογράφηση των πληροφοριών αυτών, ο χρήστης πρέπει να εισάγει τον σωστό μυστικό κωδικό. Τέλος, αν ο κωδικός είναι σωστός, η εφαρμογή αποκρυπτογραφεί τις πληροφορίες και εξάγει το αρχείο txt πατώντας το κουμπί “Extract File” (Screenshot 7).

Screenshot 7 Επιτυχής αποκρυπτογράφηση και εξαγωγή αρχείου

Κεφάλαιο 4: Συσκευές ασφαλείας

4.1 Εισαγωγή

Στα προηγούμενα κεφάλαια, αναλύσαμε, πώς θωρακίζεται ένας προσωπικός υπολογιστής στο επίπεδο του λειτουργικού συστήματος, και στη συνέχεια γνωρίσαμε τις κυριότερες τεχνικές κρυπτογράφησης δεδομένων. Παρακάτω θα προσθέσουμε ένα επιπλέον επίπεδο ασφαλείας με τη χρήση περιφερειακών συσκευών ασφαλείας (security tokens), οι οποίες απαιτούν την πιστοποίηση του χρήστη πριν από οποιαδήποτε ενέργεια. Η πιστοποίηση αυτή γίνεται μέσω χρήσης ή ακόμα και απλής κατοχής αυτών των φυσικών συσκευών.

Πρέπει να σημειώσουμε εδώ, ότι όλες αυτές οι συσκευές, λειτουργούν με το απαραίτητο συνοδευτικό λογισμικό, το οποίο και πρέπει να εγκατασταθεί στον εκάστοτε προσωπικό υπολογιστή (12).

Παρακάτω θα παρουσιάσουμε και θα εξηγήσουμε τις πιο διαδεδομένες από αυτές, που αφορούν προσωπικούς υπολογιστές.

4.2 Συσκευές κωδικού μιας χρήσης (OTP Tokens)

Οι κωδικοί μιας χρήσης είναι έγκυροι μόνο για μια πιστοποίηση/εξουσιοδότηση χρήστη. Με αυτόν τον τρόπο ακόμα και η υποκλοπή ενός τέτοιου κωδικού δεν δημιουργεί πρόβλημα ασφάλειας, καθώς ο κωδικός αυτός δεν θα είναι έγκυρος στην επόμενη πιστοποίηση.

Οι κωδικοί αυτοί παρέχονται στον χρήστη, από μια συσκευή ασφαλείας (Εικόνα 5), που παράγει κωδικούς μιας χρήσης μέσω ενός αλγορίθμου και τους εμφανίζει στην οθόνη της. Συνήθως οι συσκευές αυτές διαθέτουν ένα ακριβές ρολόι που είναι συγχρονισμένο με τον ρολόι του υπολογιστή πιστοποίησης (στην περίπτωση μας το pc του χρήστη), και παρέχουν κωδικούς βάσει χρόνου. Διαφορετικά μπορεί να παρέχουν κωδικούς βάσει ενός μαθηματικού αλγορίθμου. Τέλος το συνοδευτικό λογισμικό αναλαμβάνει να πιστοποιήσει ή όχι τον χρήστη βάσει των κωδικών που εισάγει και οι οποίοι ελέγχονται με μία εκ των προαναφερόμενων τεχνικών (13).

Εικόνα 5 Συσκευή κωδικού μιας χρήσης

Όλες οι συσκευές ασφαλείας είναι πιθανό να εμφανίσουν κάποιες αδυναμίες ή να είναι ευάλωτες σε κάποιο συγκεκριμένο είδος επιθέσεων. Οι συσκευές τύπου OTP είναι ευάλωτες σε τεχνικές ψαρέματος (τεχνική υποκλοπής πληροφοριών κατά την οποία ο εισβολέας «μεταμφιέζεται» ως αξιόπιστη οντότητα σε μια ηλεκτρονική συνομιλία για να υποκλέψει προσωπικά δεδομένα). Χαρακτηριστικό παράδειγμα τέτοιου είδους επίθεσης ήταν η υποκλοπή κωδικών OPT από μια Σουηδική τράπεζα το 2005 (14). Αν λοιπόν κάποιος εισβολέας καταφέρει να υποκλέψει ένα χρονο-προγραμματιζόμενο κωδικό μιας χρήσης, υπάρχει πιθανότητα να προλάβει να τον χρησιμοποιήσει άμεσα πριν αυτός αλλάξει. Ενώ σε περίπτωση χρήσης μαθηματικού αλγορίθμου παραγωγής κωδικών, η υποκλοπή δύο ή περισσότερων κωδικών είναι πιθανό να οδηγήσει τον υποκλοπέα σε ανακάλυψη του αλγορίθμου παραγωγής των κωδικών (νεότερες και πιο περίπλοκες υλοποιήσεις μαθηματικών αλγόριθμων μπορεί να είναι ανθεκτικότερες).

4.3 Πιστοποίηση διπλού παράγοντα (2FA)

Ένας πολύ διαδεδομένος τρόπος πιστοποίησης χρήστη είναι η πιστοποίηση διπλού παράγοντα (Two Factor Authentication) (15), κατά την οποία η εξουσιοδότηση απαιτεί δύο διαφορετικά είδη «αποδεικτικών στοιχείων». Το ένα αποδεικτικό στοιχείο είναι κάτι που ο χρήστης γνωρίζει, και το δεύτερο κάτι που έχει στην κατοχή του. Πρακτικά δηλαδή, ο χρήστης, για να πιστοποιήσει την ταυτότητα του, χρησιμοποιεί ένα σταθερό κωδικό ($1^{ος}$ παράγοντας) γνωστό σε αυτόν μαζί με έναν κωδικό που προέρχεται από μια συσκευή ασφαλείας ($2^{ος}$ παράγοντας).

Ο κωδικός του χρήστη ελέγχεται μαζί με τον κωδικό της συσκευής, από το συνοδευτικό λογισμικό, και αν ο συνδυασμός τους είναι σωστός η πιστοποίηση του χρήστη είναι επιτυχής. Επιπλέον τα δεδομένα που βρίσκονται στη συσκευή είναι κωδικοποιημένα για περισσότερη ασφάλεια.

Ανάλογα με το είδος τις συσκευής που παρέχει το δεύτερο κλειδί έχουμε τις παρακάτω κατηγορίες.

1. Συσκευές ασφαλείας USB (USB Tokens): απλά συνδέονται σε μια θύρα USB του υπολογιστή (Εικόνα 6.α).
2. Έξυπνες κάρτες (Smart Cards): απαιτούν σύνδεση card reader στον υπολογιστή για να είναι δυνατή η ανάγνωση τους (Εικόνα 6.β).
3. Ασύρματες συσκευές ασφαλείας (Wireless Tokens): συνδέονται αυτόματα με τον υπολογιστή όταν ο χρήστης βρίσκεται εντός εμβέλειας δικτύου.
4. Εικονικές συσκευές (Virtual Tokens): ένας ακόμα τρόπος είναι το δεύτερο κλειδί να παρέχεται στον χρήστη μέσω διαδικτύου από μια εταιρία ασφαλείας. Είναι οι μόνες μη φυσικές συσκευές και απαιτούν συνεχή σύνδεση στο διαδίκτυο.

Λόγω τις ποικιλίας των συσκευών ασφαλείας διπλού παράγοντα, η ευαισθησία τους σε επιθέσεις μπορεί να διαφέρει σημαντικά. Συσκευές τέτοιου τύπου που δεν κρυπτογραφούν τους κωδικούς που έχουν αποθηκευμένους μέσα τους, είναι εξαιρετικά ευαίσθητες σε περιπτώσεις κλοπής ή προσωρινής κατοχής της συσκευής από κάποιον υποκλοπέα. Σε διαφορετική περίπτωση αν ένας υποκλοπέας καταφέρει να έχει πρόσβαση στον υπολογιστή μέσω κάποιας αδυναμίας λειτουργικού συστήματος ή λογισμικού, μπορεί απλά να χρησιμοποιήσει την συνδεδεμένη συσκευή με την ιδιότητα του χρήστη και να διαβάσει τους αποθηκευμένους κωδικούς της

ακόμα και αν αυτή διαθέτει κρυπτογραφημένα δεδομένα. Ένα πρόσφατο παράδειγμα επίθεσης, αποτελεί η υποκλοπή δεδομένων, από την εταιρία παραγωγής προϊόντων ασφαλείας RSA, που αφορούν το σύστημα ελέγχου διπλού παράγοντα SecureID (16).

Εικόνα 6 α) Συσκευή ασφαλείας USB **β) Smart Card και Card Reader**

4.4 Βιομετρικοί σαρωτές

Οι Βιομετρικοί σαρωτές είναι συσκευές πιστοποίησης χρήστη και διαθέτουν έναν ή περισσότερους αισθητήρες κάποιου τύπου (οπτικό, υπέρυθρων, υπέρηχων) που λειτουργούν ως σαρωτές και μέσω των οποίων έχουν την δυνατότητα να αναλύουν διάφορα βιομετρικά χαρακτηριστικά του ανθρώπου. Η εξουσιοδότηση λοιπόν του χρήστη γίνεται βάση αποδεικτικών στοιχείων που δηλώνουν κάτι που ο χρήστης «είναι». Τα χαρακτηριστικά αυτά, όπως θα δούμε αναλυτικά παρακάτω, είναι συνήθως μοναδικά σε κάθε άνθρωπο καθιστώντας τέτοιου είδους μετρήσεις ιδανικές για ταυτοποίηση. Οι βιομετρικοί αυτοί σαρωτές έχουν την δυνατότητα να λαμβάνουν, να αποθηκεύουν και να συγκρίνουν βιομετρικές μετρήσεις σε πραγματικό χρόνο με σκοπό την πιστοποίηση της ταυτότητας του χρήστη που ζητάει πρόσβαση.

Ο πρώτος έλεγχος για την πιστοποίηση του χρήστη συνήθως γίνεται κατά την είσοδο στο λειτουργικό σύστημα, αλλά μπορούμε να συνδυάσουμε τη χρήση αυτών των συσκευών και με άλλες εφαρμογές, που καλύπτουν τις προϋποθέσεις του κατασκευαστή, μέσω του συνοδευτικού λογισμικού.

4.4.1 Βιομετρικός σαρωτής δακτυλικού αποτυπώματος

Ο Βιομετρικός σαρωτής δακτυλικού αποτυπώματος (Εικόνα 7), χρησιμοποιεί έναν οπτικό σαρωτή ή σαρωτή υπέρηχων, για να διαβάζει και να αποθηκεύει δακτυλικά αποτυπώματα σε μια βάση δεδομένων. Στη συνέχεια εφαρμόζει αλγόριθμο αναγνώρισης προτύπων ή ένα αλγόριθμο λεπτολογίας (μεθοδολογία αναγνώρισης αποτυπωμάτων), για να συγκρίνει το δακτυλικό αποτύπωμα στον σαρωτή με τα αποδεκτά δακτυλικά αποτυπώματα που είναι αποθηκευμένα στην βάση δεδομένων και να πιστοποιήσει την ταυτότητα του χρήστη (17).

Εικόνα 7 Βιομετρικός σαρωτής δακτυλικού αποτυπώματος

Είναι το πιο διαδεδομένο είδος βιομετρικού ελέγχου σε οικιακούς χρήστες λόγω του σχετικά χαμηλού κόστους και της ευχρηστίας του. Αφού ο χρήστης συνδέσει τη συσκευή με τον υπολογιστή και εγκαταστήσει το συνοδευτικό λογισμικό, ρυθμίζει τα αποδεκτά δακτυλικά αποτυπώματα. Πολλές εταιρίες παραγωγής laptop ήδη κυκλοφορούν στην αγορά μοντέλα με ενσωματωμένο βιομετρικό σαρωτή δακτυλικού αποτυπώματος (Εικόνα 8).

Εικόνα 8 Σαρωτής δακτυλικού αποτυπώματος ενσωματωμένος σε laptop

Οι αδυναμίες ασφαλείας τέτοιων συσκευών έχουν να κάνουν κυρίως με την αντιγραφή του δακτυλικού αποτυπώματος του χρήστη. Αν κάποιος υποκλοπέας καταφέρει να λάβει, με κάποιον τρόπο, το κατάλληλο δακτυλικό αποτύπωμα του χρήστη τότε μπορεί εύκολα να δημιουργήσει ένα αντίγραφο σε καλούπι ή σε μια μεμβράνη ξεγελώντας έτσι την συσκευή. Επίσης σε κάποιες περιπτώσεις είναι δυνατό ο υποκλοπέας να χρησιμοποιήσει το αποτύπωμα που δημιουργείται από τα υπολείμματα/ακαθαρσίες που αφήνει το δάκτυλο του χρήστη πάνω στον σαρωτή της συσκευής, για να αποκτήσει πρόσβαση επαναλαμβάνοντας την σάρωση. Η μελέτη «Fooling Fingerprint Scanners - Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner» (18), αναφέρεται αναλυτικά σε διάφορες αδυναμίες βιομετρικών σαρωτών δακτυλικού αποτυπώματος.

4.4.2 Βιομετρικός σαρωτής παλάμης

Ο βιομετρικός σαρωτής παλάμης χρησιμοποιεί έναν οπτικό σαρωτή ή ένα σαρωτή υπέρυθρων μέσω του οποίου λαμβάνει διάφορες μετρήσεις όπως το μήκος, το πλάτος, το πάχος αλλά και την αναλογία της παλάμης για να πιστοποιήσει τον χρήστη. Επειδή όμως αυτές οι μετρήσεις μπορεί να μην είναι αποκλειστικά μοναδικές σε έναν άνθρωπο όπως το δακτυλικό αποτύπωμα ή η ίριδα του ματιού, συνοδεύονται με ένα μοναδικό κωδικό γνωστό στο χρήστη (Εικόνα 9).

Παρόμοια με το σαρωτή δακτυλικού αποτυπώματος, οι αδυναμίες ασφαλείας της συσκευής απαιτούν την δημιουργία αντίγραφου της παλάμης του χρήστη από τον υποκλοπέα. Η λύση αυτή προσφέρει τα ίδια επίπεδα ασφάλειας και ευχρηστίας με τον σαρωτή δακτυλικού αποτυπώματος με ίσως λίγο υψηλότερο κόστος.

Εικόνα 9 Βιομετρικός σαρωτής παλάμης

Πιο προηγμένες συσκευές τέτοιου είδους (Εικόνα 10.α) είναι εξοπλισμένες με σαρωτή παλάμης και σαρωτή δακτυλικών αποτυπωμάτων, ενώ η ακρίβεια των αισθητήρων σε κάποιες υλοποιήσεις, μπορεί να καταγράψει μέχρι και τις φλέβες της παλάμης. Συνδυάζοντας τις μετρήσεις των δύο προαναφερόμενων σαρωτών, οι συσκευές αυτές δημιουργούν ένα πραγματικά μοναδικό χάρτη παλάμης για την πιστοποίηση του χρήστη (Εικόνα 10.β). Το κόστος τους όμως είναι υψηλό για τα δεδομένα του οικιακού χρήστη ενώ απαιτούν και εγκατάσταση στον χώρο. Προς το παρόν χρησιμοποιούνται κυρίως από εταιρίες και σε εφαρμογές όπου η ασφάλεια θεωρείται εξαιρετικά σημαντική.

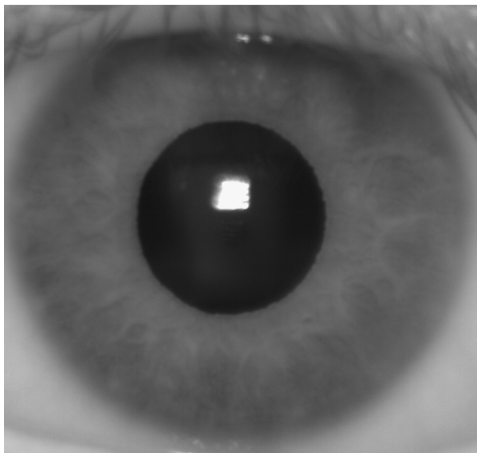
Εικόνα 10 α) Συνδυαστικός βιομετρικός σαρωτής παλάμης β) Έλεγχος παλάμης και δακτυλικών αποτυπωμάτων

4.4.3 Βιομετρικός σαρωτής ίριδας

Ο βιομετρικός σαρωτής ίριδας (Εικόνα 11.α) χρησιμοποιεί μια κάμερα υψηλής ευκρίνειας με υπέρθυρο φωτισμό για να μειώσει τις αντανακλάσεις του

φωτός στο μάτι καταγράφοντας περισσότερες πληροφορίες. Η κάμερα με αυτόν τον τρόπο μπορεί και αποτυπώνει με πολύ λεπτομερείς εικόνες τις σχηματικές δομές της ίριδας του ματιού (Εικόνα 11.β). Το συνοδευτικό λογισμικό εφαρμόζει τεχνικές αναγνώρισης προτύπων στις εικόνες αυτές, και σε σύγκριση με τα αποτυπώματα ίριδας που είναι αποθηκευμένα στην βάση δεδομένων πιστοποιεί την ταυτότητα του χρήστη (19).

Μια ευαισθησία ασφαλείας του βιομετρικού σαρωτής ίριδας είναι η αδυναμία αναγνώρισης του είδους του υλικού πάνω στο οποίο γίνονται οι μετρήσεις. Υπάρχει δηλαδή πιθανότητα ένας υποκλοπέας να καταφέρει να ξεγελάσει την συσκευή χρησιμοποιώντας μια εικόνα υψηλής ευκρίνειας του ματιού του χρήστη. Οι συσκευές αυτές προσφέρουν υψηλό επίπεδο ασφάλειας, ευκολία εγκατάστασης και χρήσης, με μεσαίο κόστος. Η μελέτη «Analysis of Vulnerabilities of Iris Scanning Personal Authentication» (20), αναφέρεται αναλυτικά σε διάφορες αδυναμίες βιομετρικών σαρωτών ίριδας.



Εικόνα 11 α) Βιομετρικός σαρωτής ίριδας **β) Αποτύπωμα ίριδας**

4.4.4 Βιομετρικός σαρωτής προσώπου

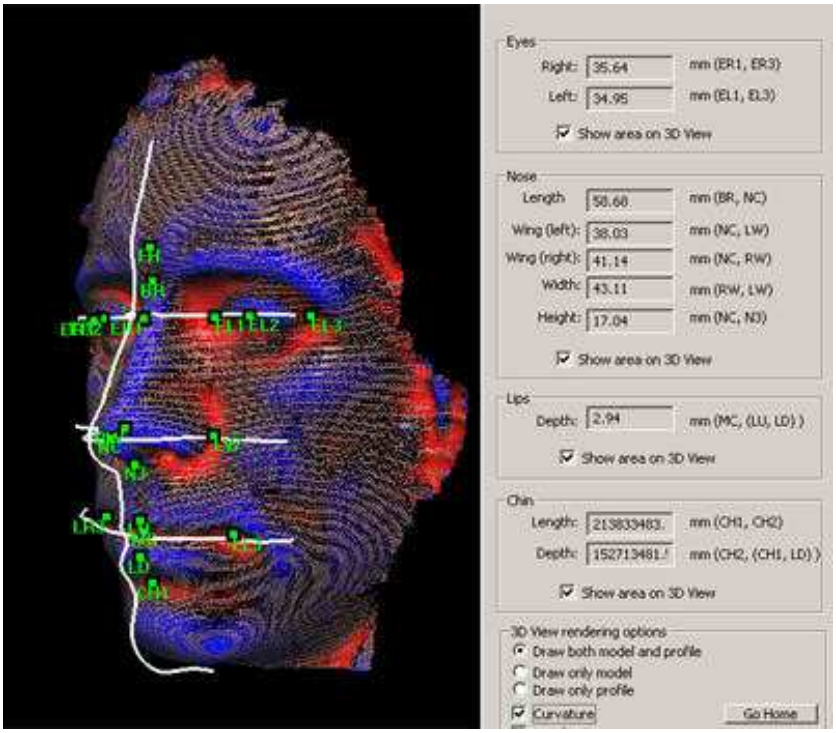
Ο βιομετρικός σαρωτής προσώπου (Εικόνα 12) χρησιμοποιεί μια ή περισσότερες κάμερες υψηλής ευκρίνειας για να αποτυπώσει με λεπτομερείς εικόνες ολόκληρο το πρόσωπο. Η πιστοποίηση γίνεται μέσω αλγορίθμων που συγκρίνουν επιλεκτικά τα χαρακτηριστικά του προσώπου, δηλαδή τη σχετική θέση, το μέγεθος και το σχήμα που έχουν τα μάτια, η μύτη και το στόμα στο πρόσωπο. Αν ο συνδυασμός των προαναφερόμενων μετρήσεων συμπίπτει με τις μετρήσεις που προϋπάρχουν στην βάση δεδομένων προσώπων, η πιστοποίηση είναι επιτυχής.

Όπως και στον βιομετρικό σαρωτή ίριδας, είναι αδύνατη η αναγνώριση του υλικού που σαρώνεται από τους αισθητήρες. Ειδικότερα, υλοποιήσεις που διαθέτουν μία κάμερα, είναι πιθανό να παρακαμφθούν με τη χρήση φωτογραφιών υψηλής ευκρίνειας του προσώπου ενός αποδεκτού χρήστη, σε συνδυασμό βέβαια με υποκλοπή του κωδικού του. Μια αντίστοιχη περίπτωση, που αφορά φορητούς υπολογιστές, αναφέρεται στο άρθρο «Laptop face-recognition tech easy to hack, warns Black Hat researcher» (21). Η διάδοση τέτοιων συσκευών σε οικιακούς χρήστες είναι σε πρώιμα στάδια λόγω του υψηλού κόστους και των απαιτήσεων εγκατάστασης, προσφέρουν όμως ανάλογα υψηλό επίπεδο ασφάλειας.

Εικόνα 12 Βιομετρικός σαρωτής προσώπου με δύο κάμερες και αριθμητικό κωδικό

Οι βιομετρικοί σαρωτές προσώπου νέας τεχνολογίας χρησιμοποιούν αισθητήρες καταγραφής τρισδιάστατων αντικειμένων, τοποθετημένους σε κατάλληλες θέσεις και αποστάσεις, ώστε να λαμβάνουν και να συγκρίνουν τρισδιάστατες απεικονίσεις του προσώπου (Εικόνα 13). Επίσης μια ανερχόμενη μέθοδος που τείνει να ενσωματωθεί σε αυτές τις συσκευές είναι και η ανάλυση δερματικής υφής που θα λαμβάνει υπόψη σημάδια και γραμμές στο δέρμα. Ο συνδυασμός όλων αυτών των βιομετρικών μετρήσεων προσφέρει πολύ περισσότερες λεπτομέρειες και κατά συνέπεια πολύ μεγαλύτερο όγκο πληροφοριών για έλεγχο και αποτελεί την τελευταία λέξη της τεχνολογίας στις συσκευές πιστοποίησης χρήστη (22).

Το κόστος τέτοιων συσκευών όμως είναι εξαιρετικά υψηλό, ενώ η εγκατάσταση είναι μια πολύπλοκη διαδικασία που προϋποθέτει, μεταξύ άλλων, και μελέτη χώρου. Η χρήση τους στις μέρες μας περιορίζεται σε μεγάλες εταιρίες και οργανισμούς μόνο για εφαρμογές όπου η ασφάλεια θεωρείται εξαιρετικά σημαντική.



Εικόνα 13 Αποτύπωμα προσώπου από αισθητήρες 3D

Κεφάλαιο 5: Πλήρης κρυπτογράφηση δίσκου

Η κρυπτογράφηση δίσκου χρησιμοποιεί κατάλληλο λογισμικό ή υλικό για να κρυπτογραφήσει κάθε bit δεδομένων που βρίσκεται σε ένα δίσκο ή έναν τόμο του, με στόχο να αποτρέψει την πρόσβαση στα δεδομένα αυτά από μη εξουσιοδοτημένους χρήστες. Αλλιώς ονομάζεται πλήρης κρυπτογράφηση δίσκου, δηλώνοντας έτσι, ότι κρυπτογραφούνται σχεδόν τα πάντα σε ένα δίσκο ο οποίος λειτουργεί ως κύριος δίσκος εκκίνησης του λειτουργικού συστήματος (23).

Γενικά χωρίζονται σε δύο κατηγορίες με βάση την υλοποίηση τους:

- Πλήρης κρυπτογράφηση δίσκου με λογισμικό
- Πλήρης κρυπτογράφηση δίσκου με υλικό

5.1 Πλήρης κρυπτογράφηση δίσκου με λογισμικό

Η υλοποίηση της πλήρους κρυπτογράφησης δίσκου με λογισμικό χρησιμοποιεί έναν αλγόριθμο κρυπτογράφησης ή ένα συνδυασμό αλγορίθμων που εφαρμόζονται σταδιακά, για την κρυπτογράφηση όλων των δεδομένων στον δίσκο με το ίδιο κλειδί, σε επίπεδο λογισμικού. Στα μειονέκτημα της είναι το ότι αδυνατεί να κρυπτογραφήσει το πεδίο MBR των δίσκων. Το MBR περιέχει δεδομένα απαραίτητα για την εκκίνηση του λειτουργικού συστήματος, και πληροφορίες που περιγράφουν τις μονάδες στις οποίες ο δίσκος είναι χωρισμένος, αφήνοντας έτσι ένα μικρό αλλά σημαντικό κομμάτι του δίσκου ευάλωτο.

Υπάρχει μια ποικιλία τέτοιων προγραμμάτων στην αγορά που χρησιμοποιούν διαφορετικούς αλγόριθμους. Πέρα από το BitLocker της Microsoft που έχουμε προαναφέρει, υπάρχει το Symantec Endpoint Encryption Full Disk Encryption αλλά και το δωρεάν TrueCrypt (7) που θα εφαρμόσουμε στο επόμενο κεφάλαιο.

5.2 Πλήρης κρυπτογράφηση δίσκου με υλικό

Σε αυτήν την κατηγορία η πλήρης κρυπτογράφηση δίσκου γίνεται μέσω υλικού (hardware), που σε συνδυασμό με το συνοδευτικό του λογισμικό, υλοποιεί κάποιες τεχνικές ασφαλείας. Παρακάτω θα δούμε δύο διαφορετικές εφαρμογές πλήρους κρυπτογράφησης δίσκου με υλικό.

5.2.1 Σκληροί δίσκοι FDE

Οι σκληροί δίσκοι FDE (Εικόνα 14) είναι διαθέσιμοι σχεδόν από όλες τις εταιρίες κατασκευής σκληρών δίσκων. Η πιστοποίηση χρήστη γίνεται κατά την ενεργοποίηση του δίσκου είτε μέσω ενός κωδικού BIOS είτε με κάποιο λογισμικό που τρέχει σε περιβάλλον προ εκκίνησης.

Ένα πλεονέκτημα τους είναι το ότι η διαχείριση των κλειδιών γίνεται από τον ελεγκτή του δίσκου και χρησιμοποιεί κρυπτογραφικά κλειδιά αλγορίθμου AES με μήκος 128 ή 256 bit. Τα κλειδιά αυτά τα αποθηκεύει και διαχειρίζεται ο δίσκος, ανεξάρτητα από τον κεντρικό επεξεργαστή, εξαλείφοντας έτσι κινδύνους που μπορούν να προέλθουν από πληροφορίες αποθηκευμένες στην μνήμη του

υπολογιστή. Τέλος άλλο ένα σημαντικό πλεονέκτημα τους είναι ότι έχουν την δυνατότητα να κρυπτογραφούν και το MBR του δίσκου (24).

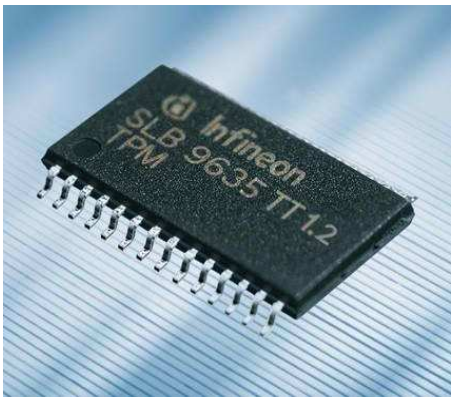
Εικόνα 14 Σκληρός Δίσκος FDE από τη Seagate

5.2.2 Κρυπτο-επεξεργαστής TPM

Το TPM ή TPM chip (Εικόνα 15) είναι ένας ασφαλής κρυπτο-επεξεργαστής ενσωματωμένος στην μητρική πλακέτα του υπολογιστή, χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού και έχει την δυνατότητα να δημιουργεί, να αποθηκεύει αλλά και να περιορίζει την χρήση κρυπτογραφικών κλειδιών.

Κάθε TPM chip έχει ένα μοναδικό ζεύγος κλειδιών αλγόριθμου RSA με μήκος 2048 bit που του αποδίδεται κατά την παραγωγή, και μέσω αυτού μπορεί να κρυπτογραφεί δεδομένα αλλά και να προσφέρει πιστοποίηση υλικού ελέγχοντας, αν η συσκευή που ζητάει πρόσβαση στο σύστημα, είναι εξουσιοδοτημένη.

Επίσης μέσω κατάλληλων διεργασιών δημιουργεί ένα hash key (κλειδί κατακερματισμού) για ολόκληρο το σύστημα, το οποίο αντιπροσωπεύει το σύνολο της σύνθεσης λογισμικού και υλικού του υπολογιστή και είναι ουσιαστικά αδύνατο να πλαστογραφηθεί. Με αυτό τον τρόπο μπορεί να πιστοποιεί την ακεραιότητα λογισμικού και υλικού, αναγνωρίζοντας οποιαδήποτε μη εξουσιοδοτημένη τροποποίηση τους (25).



Εικόνα 15 TPM Chip

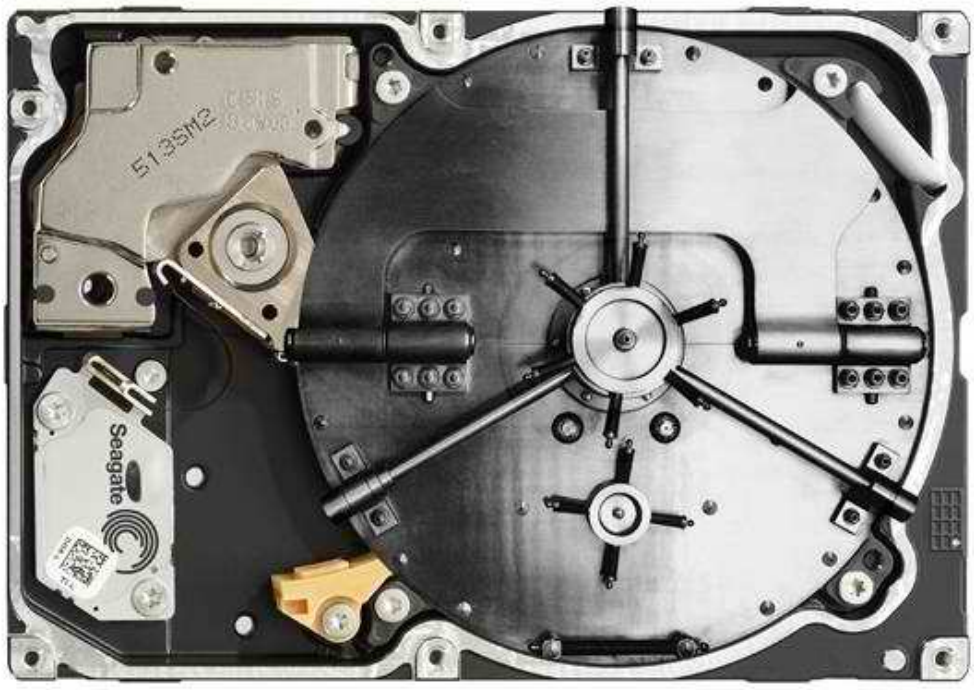
5.3 Ανάπτυξη τεχνολογιών ασφάλειας υπολογιστών

Αντιλαμβανόμενες την ολοένα αυξανόμενη ανάγκη για ασφάλεια, οι μεγαλύτερες εταιρίες στον χώρο της πληροφορικής, και πιο συγκεκριμένα οι AMD, Hewlett-Packard, IBM, Intel και Microsoft συνέπραξαν στην δημιουργία του Trusted Computing Group ή TCG (26), ενός μη κερδοσκοπικού οργανισμού με στόχο να αναπτύξει βιομηχανικά πρότυπα παραγωγής ασφαλούς και έμπιστου υλικού υπολογιστών και το λογισμικό περιβάλλον για αυτά. Στην σύμπραξη αυτή εισχώρησαν πολλές ακόμα εταιρίες με την πάροδο των χρόνων.

Ο πρώτος στόχος του TCG ήταν η δημιουργία του TPM chip που περιγράψαμε παραπάνω. Επίσης προσφάτως το TCG κυκλοφόρησε την πρώτη έκδοση του πρωτοκόλλου προδιαγραφών TNC με δυνατότητα να πιστοποιεί τους χρήστες ενός δικτύου με βάση τις προδιαγραφές υλικού που έχουν.

Πιο πρόσφατα το 2009, το TCG και πιο συγκεκριμένα ένας υποκλάδος, του ονόματι SWG, κυκλοφόρησε το Trusted Storage Architecture Core Specification, ένα σετ προδιαγραφών που περιγράφει το πρωτόκολλο επικοινωνίας με αυτό-κρυπτογραφούμενους σκληρούς δίσκους, και το SSC που περιγράφει τις απαιτήσεις κάθε κατηγορίας τέτοιων συσκευών. Το Enterprise SSC ορίζει τις ελάχιστες απαιτήσεις συσκευών για servers και data centers, ενώ το Opal SSC ορίζει τις ελάχιστες απαιτήσεις για συσκευές σε προσωπικούς υπολογιστές (27).

Οι νέοι σκληροί δίσκοι που ενσωματώνουν αυτή την τεχνολογία του TCG υλοποιώντας το Opal SSC ονομάζονται σκληροί δίσκοι SED (Εικόνα 16) και τα πρώτα μοντέλα ξεκίνησαν να κυκλοφορούν στην αγορά το 2010.



Εικόνα 16 Σκληρός Δίσκος SED από την Seagate

Αν και η TCG είναι μη κερδοσκοπική και έχει ως στόχο, όπως δηλώνει και η ίδια, να αναπτύξει πρότυπα που προσφέρουν περισσότερη ασφάλεια στους χρήστες, έχει δεχτεί πολλή κριτική με την πάροδο των χρόνων από την κοινότητα ελεύθερου λογισμικού αλλά και τις κοινότητες των λειτουργικών συστημάτων Linux και FreeBSD. Οι εν λόγω κοινότητες μαζί και με άλλες εταιρίες παραγωγής λογισμικού, κατηγορούν την TCG για δόλιες πρακτικές με απώτερο σκοπό τον πλήρη έλεγχο του λογισμικού.

Θεωρούν δηλαδή ότι οι τεχνολογίες που αναπτύσσει η TCG σε συνδυασμό με λογισμικό όπως το DRM, που χρησιμοποιείται από τις μεγαλύτερες εταιρίες παραγωγής λογισμικού και έχει τη δυνατότητα να αποτρέπει την χρήση του ψηφιακού περιεχόμενου που αγοράζει ο κάθε χρήστης, με οποιοδήποτε τρόπο, πέραν του προβλεπόμενου, από την εταιρία παραγωγής, θα επιτρέψουν τελικά στους κατασκευαστές να αποκλείουν την εγκατάσταση οποιουδήποτε λογισμικού δεν είναι επίσημα πιστοποιημένο από τους ίδιους, καθιστώντας το άχρηστο.

Συμπερασματικά η TCG υποστηρίζεται από τους περισσότερους κατασκευαστές υλικού ειδικά στην κατηγορία των σκληρών δίσκων, και τα προϊόντα που εφαρμόζουν τα πρότυπα της έχουν ενσωματωμένες κρυπτογραφικές δυνατότητες που προσφέρουν ένα επιπλέον επίπεδο ασφάλειας δεδομένων, το οποίο δεν μπορεί να επιτευχθεί με κρυπτογράφηση λογισμικού. Το μέλλον μόνο μπορεί να δείξει πώς και προς τα πού θα εξελιχθούν τέτοιου είδους τεχνολογίες και αν τελικά η χρήση τους επιβάλει άλλους μη επιθυμητούς περιορισμούς στους χρήστες εκτός της υψηλής ασφάλειας που προσφέρουν σήμερα.

Κεφάλαιο 6: Εφαρμογή πλήρους κρυπτογράφησης δίσκου

6.1 Επιλογή λογισμικού

Στο κεφάλαιο αυτό θα εξετάσουμε την πρακτική εφαρμογή λογισμικού πλήρους κρυπτογράφησης δίσκου, χρησιμοποιώντας το απαραίτητο λογισμικό. Όπως έχουμε προαναφέρει υπάρχει μεγάλη ποικιλία τέτοιου είδους λογισμικού. Ενδεικτικά αναφέρονται μερικά από αυτά:

- BitLocker: Λογισμικό ενσωματωμένο στις εκδόσεις Windows Business και Ultimate που χρησιμοποιεί αλγόριθμο AES για πλήρη κρυπτογράφηση δίσκου (28).
- CenterTools DriveLock Suite: Προσφέρει κρυπτογράφηση δεδομένων και πλήρη κρυπτογράφηση δίσκου με χρήση αλγόριθμων συμμετρικού κλειδιού επιλογής του χρήστη (AES, 3DES, Blowfish κ.α.) (29).
- McAfee Endpoint Encryption: Εκτός από κρυπτογράφηση δεδομένων και πλήρη κρυπτογράφηση δίσκου διαθέτει ενσωματωμένο και λογισμικό ελέγχου πρόσβασης με δύο ή τρείς παράγοντες πιστοποίησης. Εκτός από Windows υποστηρίζει και λειτουργικό σύστημα Mac (30).
- PGP Whole Disk Encryption από την Symantec: Προσφέρει ισχυρή κρυπτογραφία δεδομένων και πλήρη κρυπτογράφηση σκληρού δίσκου υψηλής απόδοσης, με τη χρήση αλγορίθμων δημοσίου κλειδιού που ονομάζονται PGP HCO. Υποστηρίζει λειτουργικά συστήματα Windows, Mac και Linux (31).
- TrueCrypt: Δωρεάν λογισμικό που προσφέρει κρυπτογράφηση δεδομένων και πλήρη κρυπτογράφηση δίσκου, με χρήση αλγόριθμων συμμετρικού κλειδιού επιλογής του χρήστη.

Η επιλογή μας είναι το δωρεάν λογισμικό TrueCrypt (7), ένα λογισμικό ανοιχτού πηγαίου κώδικα (open-source software), ελεύθερο προς μελέτη και τροποποίηση, που μπορεί να χρησιμοποιηθεί για εκπαιδευτικούς σκοπούς ενώ υποστηρίζει και όλες τις σύγχρονες εκδόσεις λειτουργικού συστήματος Windows 32bit και 64bit (Windows Server 2003, Windows Server 2008, Windows Xp, Windows Vista και Windows 7).

6.2 Περιγραφή λειτουργίας TrueCrypt

Το TrueCrypt είναι μια εφαρμογή που χρησιμοποιεί την τεχνική της κρυπτογράφησης/αποκρυπτογράφησης σε πραγματικό χρόνο (On-the-fly encryption/decryption) για να κρυπτογραφεί και να διατηρεί την κρυπτογράφηση σε ένα τόμο δίσκου. Η τεχνική on-the-fly υποδηλώνει ουσιαστικά ότι τα δεδομένα κρυπτογραφούνται αμέσως πριν αποθηκευτούν στον τόμο και αποκρυπτογραφούνται αμέσως μόλις φορτωθούν από αυτόν, χωρίς να χρειάζεται καμία ενέργεια από τον χρήστη.

Αυτό πρακτικά σημαίνει, ότι όλα τα δεδομένα που είναι αποθηκευμένα στον τόμο του δίσκου είναι συνεχώς και πάντα κρυπτογραφημένα, ενώ η αποκρυπτογράφηση οποιουδήποτε εξ' αυτών είναι δυνατή μόνο με τη χρήση του σωστού κωδικού ή κλειδιού κρυπτογράφησης. Όταν ο χρήστης ζητάει ένα αρχείο από τον κρυπτογραφημένο τόμο, η κρυπτογραφημένη μορφή του αρχείου φορτώνεται

στην μνήμη και μετά αποκρυπτογραφείται. Αντίστροφα όταν ο χρήστης αποθηκεύει ένα αρχείο στον κρυπτογραφημένο τόμο, αυτό κρυπτογραφείται σε πραγματικό χρόνο στην μνήμη και μετά αποθηκεύεται στον δίσκο.

Πρέπει να σημειώσουμε εδώ ότι το TrueCrypt δεν απαιτεί συστήματα με επιπλέον μνήμη, αφού η διαδικασία της κρυπτογράφησης/αποκρυπτογράφησης ακόμα και σε μεγάλα αρχεία εφαρμόζεται τμηματικά.

6.3 Περιγραφή συστήματος

Η πρακτική εφαρμογή πλήρους κρυπτογράφησης δίσκου με χρήση του TrueCrypt θα γίνει σε ένα προσωπικό υπολογιστή τύπου laptop με τα εξής χαρακτηριστικά:

- Κατασκευαστής: Hewlett Packard
- Μοντέλο: HP HDX 16
- Επεξεργαστής: Intel Core 2 Duo T9400 @ 2.53GHz
- Μνήμη: 4 GB DDR2
- Σκληρός δίσκος: 320 GB 5400 rpm SATA 2
- Κάρτα γραφικών: GeForce 9600M GT
- Λειτουργικό σύστημα: Windows Vista Home Premium (SP2) 64bit

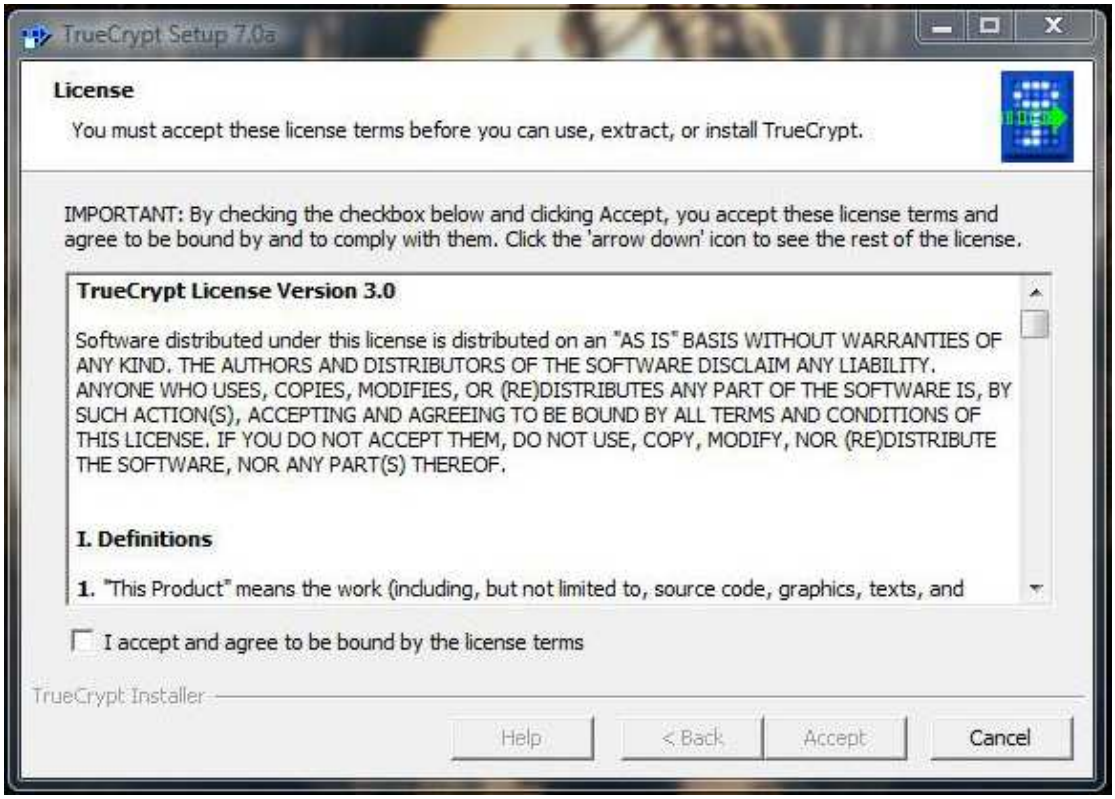
6.4 Εφαρμογή πλήρους κρυπτογράφησης δίσκου με TrueCrypt

Κατά την συγγραφή αυτής της πτυχιακής, η πιο πρόσφατη έκδοση του TrueCrypt ήταν η 7.0a σε γλώσσα αγγλική και με ημερομηνία έκδοσης 6 Σεπτεμβρίου 2010. Αυτή την έκδοση χρησιμοποιούμε και στην παρακάτω εκτέλεση και ανάλυση λειτουργίας της εφαρμογής.

6.4.1 Εγκατάσταση TrueCrypt

Αφού έχουμε προμηθευθεί την τελευταία έκδοση του TrueCrypt από την επίσημη ιστοσελίδα του http://www.truecrypt.org/ , τρέχουμε το αρχείο εγκατάστασης της εφαρμογής και ακολουθούμε τις οδηγίες:

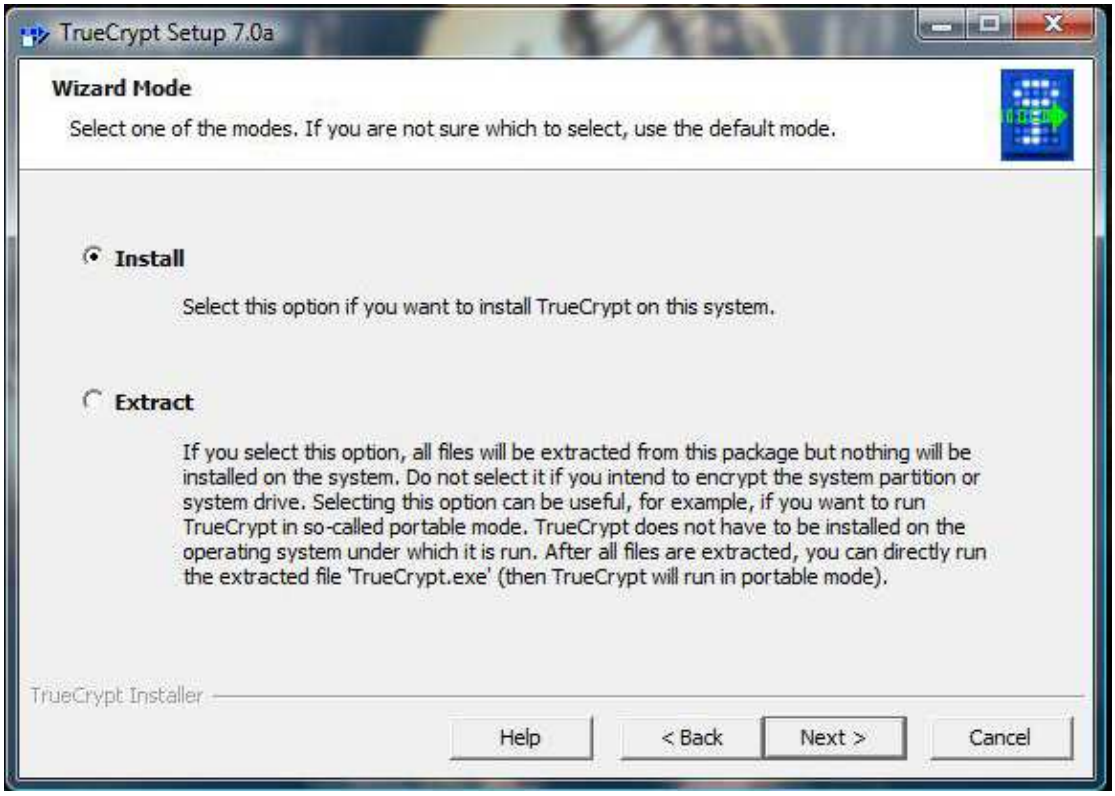
1^{ο} Βήμα: Διαβάζουμε τους όρους και αποδεχόμαστε την άδεια χρήσης (license agreement) της εφαρμογής (Screenshot 8).



Screenshot 8 Άδεια χρήσης

2ο Βήμα: Επιλέγουμε την κατάσταση λειτουργίας της εφαρμογής (Screenshot 9) έχοντας δύο επιλογές:

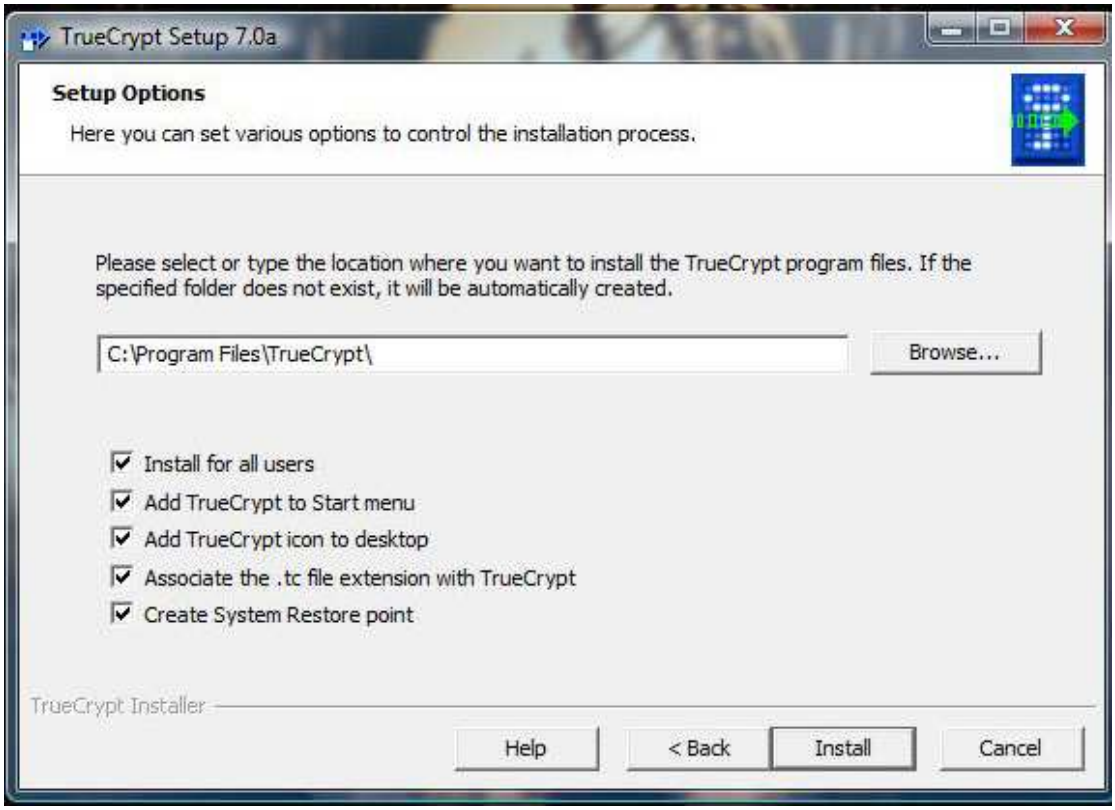
1) Εγκατάσταση εφαρμογής: υποστηρίζει όλες τις λειτουργίες.
2) Αποσυμπίεση εφαρμογής: αποσυμπιέζει όλα τα αρχεία του πακέτου αλλά δεν εγκαθιστά τίποτα. Προτείνεται μόνο για χρήση κρυπτογράφησης μεμονωμένων αρχείων ενώ δεν υποστηρίζεται πλήρης κρυπτογράφηση δίσκου.



Screenshot 9 Κατάσταση λειτουργίας

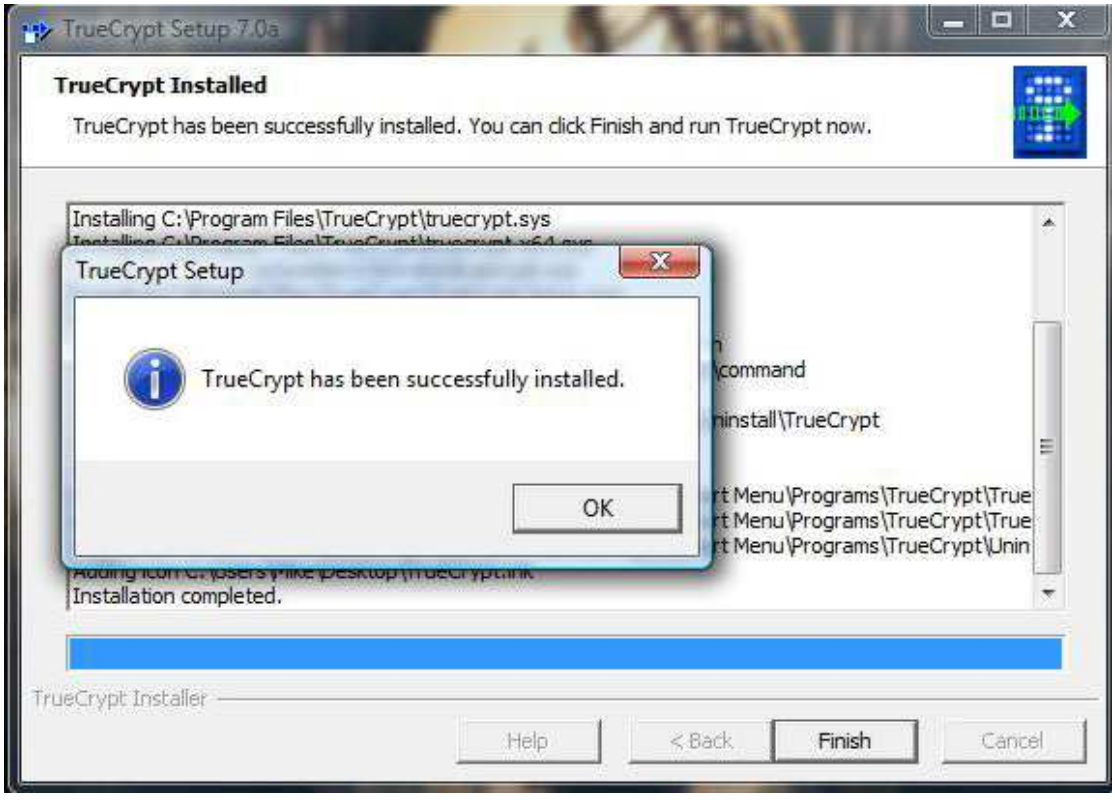
Εμείς επιθυμούμε πλήρη κρυπτογράφηση δίσκου και επιλέγουμε εγκατάσταση.

3ο Βήμα: Επιλέγουμε τον προορισμό αποθήκευσης των αρχείων της εφαρμογής, μαζί με κάποιες μικροεπιλογές χρήσης και συντομεύσεων (Screenshot 10). Το τελευταίο checkbox αναφέρει “Create System Restore Point” και προτείνεται να είναι επιλεγμένο καθώς δημιουργεί ένα σημείο ανάκτησης λειτουργικού συστήματος για χρήση από το κέντρο επαναφοράς των Windows (αναφερθήκαμε σε αυτό στο κεφάλαιο 2). Το σημείο ανάκτησης λειτουργεί ως δικλείδα ασφαλείας σε περίπτωση κάποιου απρόβλεπτου καταστροφικού προβλήματος.



Screenshot 10 Επιλογή προορισμού αποθήκευσης

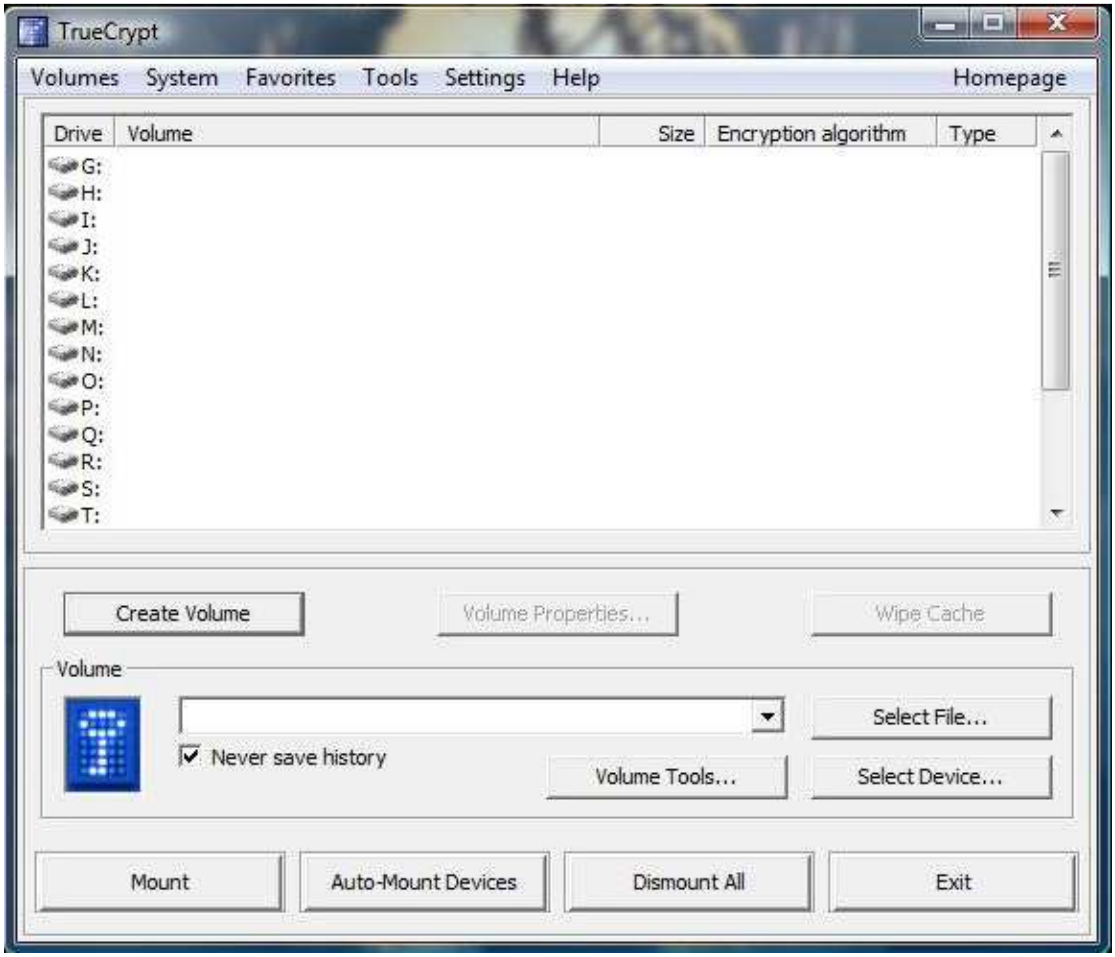
4ο Βήμα: Επιτυχής ολοκλήρωση εγκατάστασης (Screenshot 11).



Screenshot 11 Τέλος εγκατάστασης

6.4.2 Δημιουργία κρυπτογραφημένων τόμων και τρόποι χρήσης

Μετά το τέλος της εγκατάστασης τρέχουμε την εφαρμογή TrueCrypt (Screenshot 12) και πατάμε το κουμπί δημιουργίας κρυπτογραφημένου τόμου “Create Volume”.

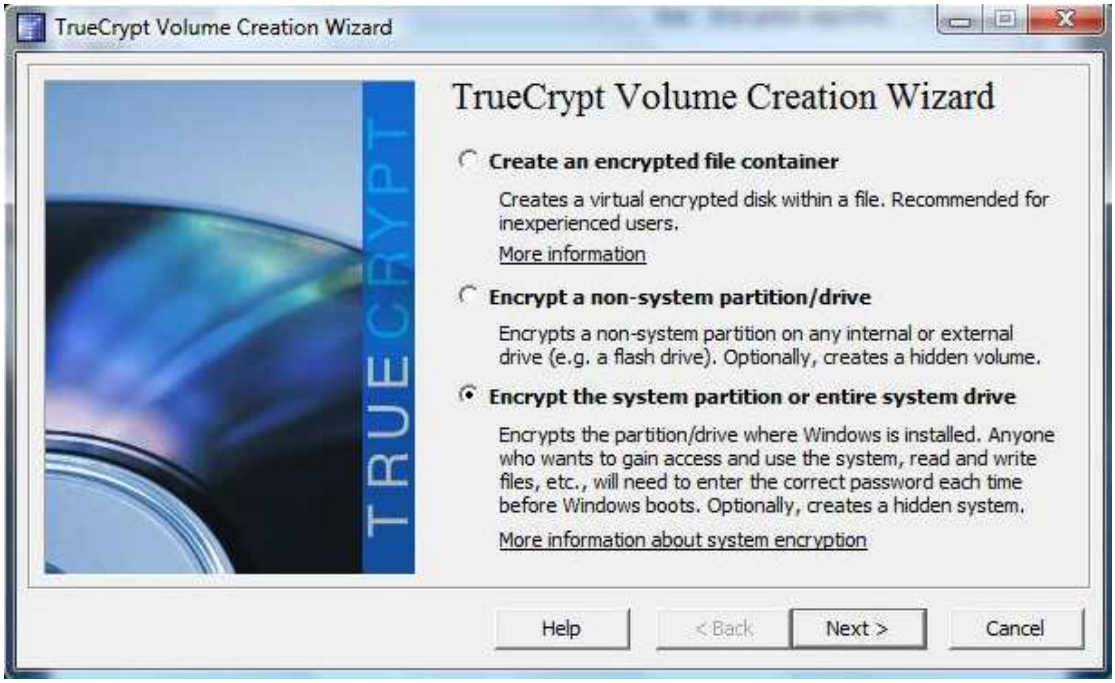


Screenshot 12 Κυρίως μενού TrueCrypt

Το TrueCrypt έχει τρείς κύριους τρόπους χρήσης και δημιουργίας κρυπτογραφημένων δίσκων/τόμων (Screenshot 13):

1. Δημιουργία κρυπτογραφημένης περιοχής.
   Πρακτικά δημιουργεί ένα κρυπτογραφημένο εικονικό δίσκο στον οποίο ο χρήστης μπορεί να αποθηκεύει, οποιαδήποτε αρχεία και γενικότερα δεδομένα, θεωρεί ο ίδιος κρίσιμα. Ουσιαστικά δηλαδή είναι ένα «θησαυροφυλάκιο» δεδομένων, όπου όλα τα δεδομένα που βρίσκονται μέσα του είναι κρυπτογραφημένα.

2. Κρυπτογράφηση δίσκου/τόμου δίσκου που δεν περιέχει λειτουργικό σύστημα.
   Κρυπτογραφεί όλα τα δεδομένα σε ένα δίσκο ή κάποιον τόμο του, με την προϋπόθεση να μην περιέχει αρχεία λειτουργικού συστήματος. Δίνει επίσης τη δυνατότητα στον χρήστη να δημιουργεί κρυφούς τόμους, δηλαδή τη δημιουργία ενός κρυφού κρυπτογραφημένου τόμου μέσα σε ένα ήδη κρυπτογραφημένο τόμο.



Screenshot 13 Επιλογή χρήσης εφαρμογής

3. Κρυπτογράφηση δίσκου/τόμου δίσκου που περιέχει λειτουργικό σύστημα. Κρυπτογραφεί όλα τα δεδομένα στον δίσκο/τόμο του λειτουργικού συστήματος που βρίσκονται τα Windows. Οποιοσδήποτε χρήστης επιθυμεί πρόσβαση και χρήση του υπολογιστή θα πρέπει να εισάγει τον σωστό κωδικό κάθε φορά που γίνεται εκκίνηση του υπολογιστή και προτού φορτώσουν τα Windows (Screenshot 14). Όπως και στον προηγούμενο τρόπο χρήσης υπάρχει η δυνατότητα δημιουργίας κρυφού τόμου λειτουργικού συστήματος μέσα σε ένα ήδη κρυπτογραφημένο τόμο για περισσότερη ασφάλεια. Θα αναφερθούμε αναλυτικότερα στους κρυφούς τόμους παρακάτω.

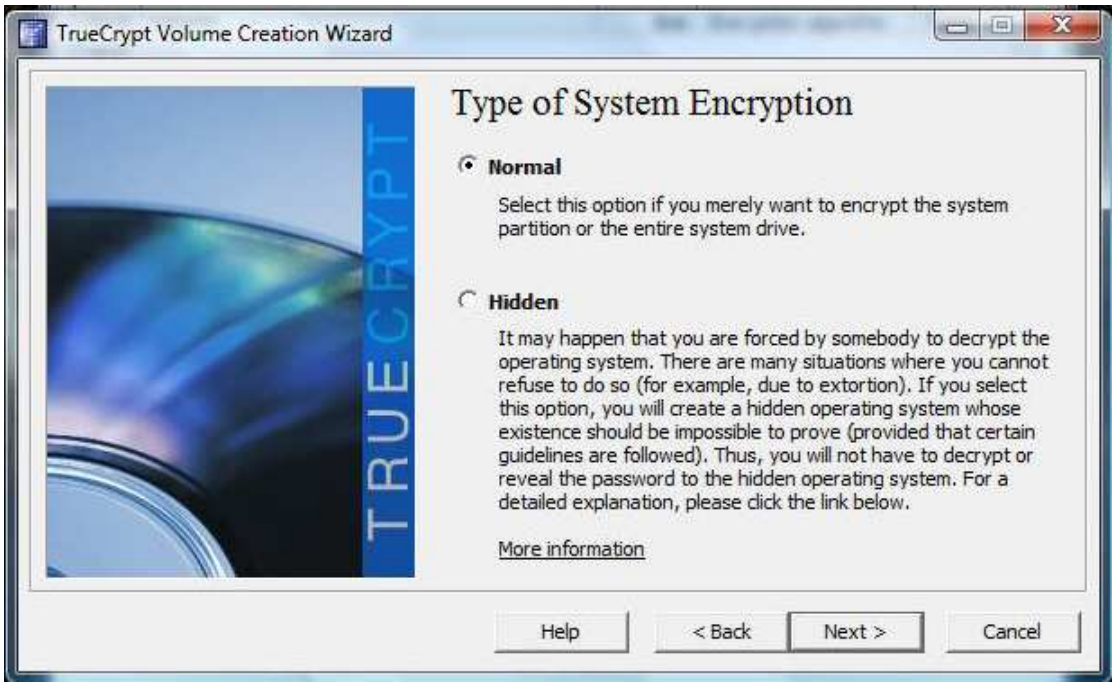
Screenshot 14 TrueCrypt Boot Loader

Εμείς επιλέξαμε τον τρίτο και πιο περίπλοκο τρόπο χρήσης καθώς η κρυπτογράφηση θα γίνει σε τόμο δίσκου που περιέχει λειτουργικό σύστημα και προχωράμε. Σημειώνουμε πάντως ότι όλες οι επιλογές που θα δούμε αναλυτικά παρακάτω ισχύουν κατά την χρήση της εφαρμογής και με τους τρείς τρόπους.

Καθώς προχωράμε βήμα προς βήμα, η εφαρμογή θα μας επιτρέψει να κάνουμε διάφορες επιλογές που αφορούν την διαδικασία, τον τρόπο και τον τύπο της κρυπτογράφησης. Παρακάτω θα δείξουμε και θα εξηγήσουμε σταδιακά αυτές τις επιλογές κάνοντας παράλληλα κάποιες διαπιστώσεις και προτάσεις προς τον χρήστη.

6.4.3 Γενικές επιλογές και δυνατότητες

1ο Βήμα: Η πρώτη επιλογή χρήστη αφορά το αν ο τόμος που θα δημιουργήσουμε θα είναι απλός ή κρυφός (Screenshot 15). Όπως προαναφέραμε κρυφοί τόμοι μπορούν να δημιουργηθούν μέσα σε ήδη κρυπτογραφημένους τόμους, και προσδίδουν έτσι ένα επιπλέον επίπεδο ασφάλειας. Ακόμα και στην περίπτωση του εξαναγκασμού/εκβιασμού του χρήστη/κάτοχου των κρυπτογραφημένων δεδομένων σε αποκάλυψη του κωδικού της πρώτης κρυπτογράφησης, δεν υπάρχει προφανής τρόπος αναγνώρισης της ύπαρξης κρυφών τόμων παρά μόνο από τον δημιουργό τους. Προτείνεται ο κωδικός ενός κρυφού τόμου να είναι εντελώς διαφορετικός σε σχέση με τον κωδικό του απλού κρυπτογραφημένου τόμου μέσα στον οποίο δημιουργείται.



Screenshot 15 Επιλογή τύπου δημιουργούμενου τόμου

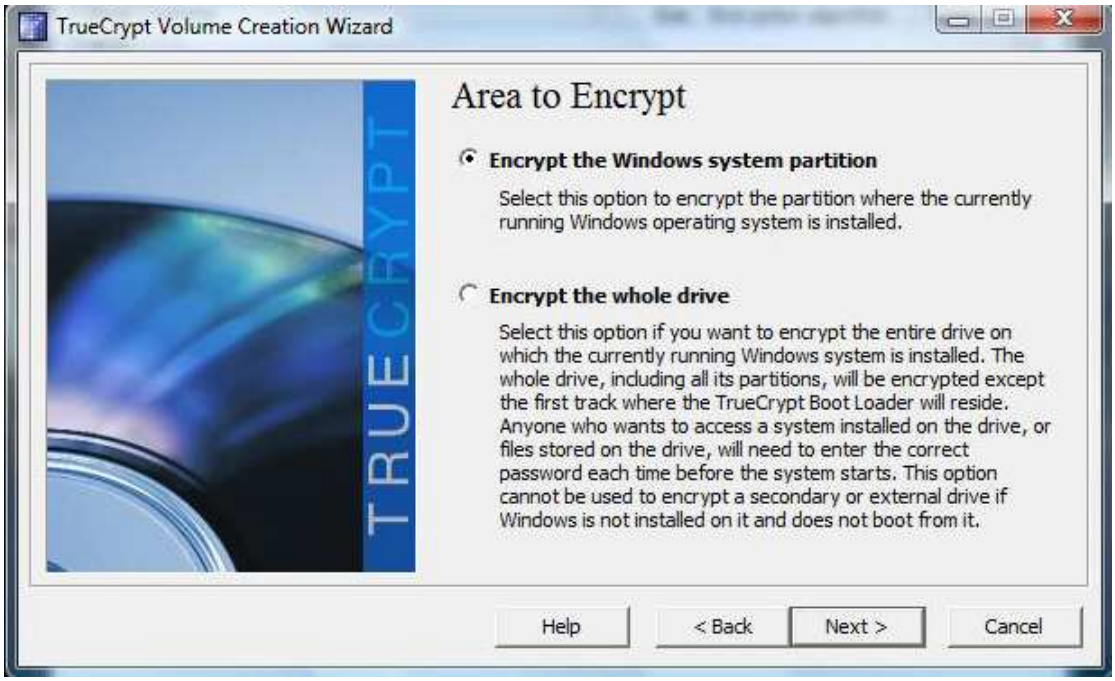
Εμείς επιλέγουμε απλό τύπο αφού δεν προϋπάρχει κρυπτογραφημένος τόμος και προχωράμε.

2ο Βήμα: Επόμενη επιλογή είναι η περιοχή του δίσκου στην οποία θα εφαρμοστεί η κρυπτογράφηση (Screenshot 16). Μπορούμε να επιλέξουμε μεταξύ:

1. Κρυπτογράφηση μόνο του τόμου στον οποίο βρίσκεται το λειτουργικό σύστημα.
2. Κρυπτογράφηση του τόμου στον οποίο βρίσκεται το λειτουργικό σύστημα και όλων των τόμων που βρίσκονται στον ίδιο δίσκο.

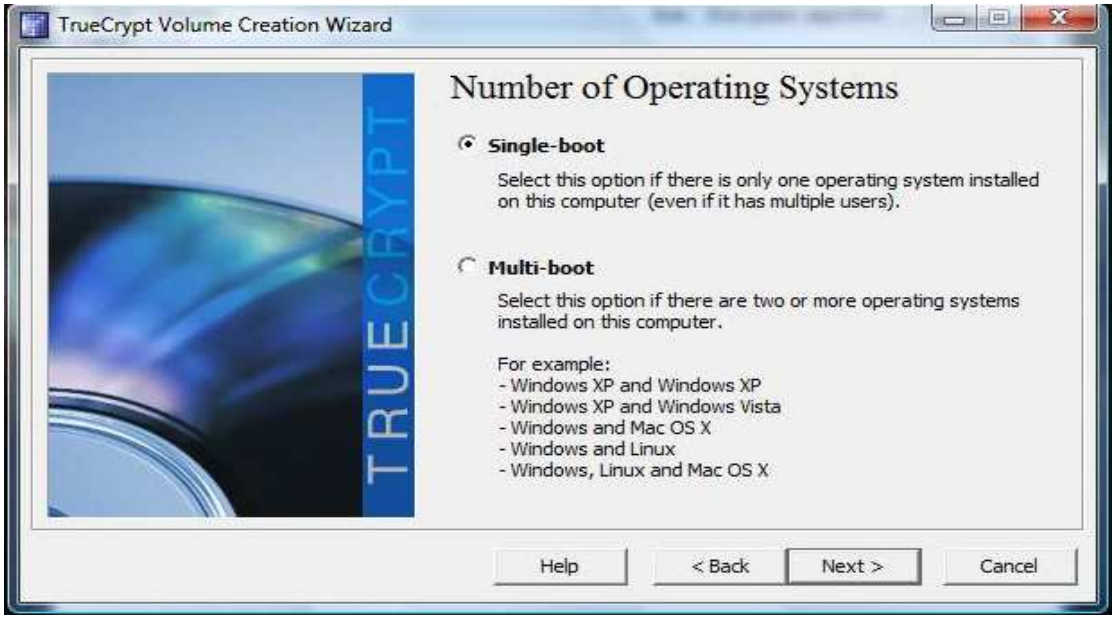
Σε αυτή την πρακτική εφαρμογή επιλέξαμε κρυπτογράφηση μόνο του τόμου στον οποίο βρίσκονται τα Windows λόγω του μεγάλου όγκου μη κρίσιμων δεδομένων στους υπόλοιπους τόμους. Αν ο χρήστης επιθυμεί πλήρη ασφάλεια όλων των

δεδομένων που μπορεί να βρίσκονται αποθηκευμένα σε οποιοδήποτε τόμο του δίσκου, προτείνεται η χρήση της επιλογής β).



Screenshot 16 Επιλογή περιοχής δίσκου προς κρυπτογράφηση

3ο Βήμα: Άλλη μια σημαντική πληροφορία αφορά το αν το σύστημα μας έχει ένα λειτουργικό σύστημα εγκατεστημένο ή περισσότερα (Screenshot 17). Υπολογιστές που διαθέτουν περισσότερα από ένα λειτουργικά συστήματα, απαιτούν ένα διαφορετικό τόμο στο δίσκο ή και διαφορετικούς δίσκους για να εγκατασταθεί καθένα από αυτά. Σε τέτοιες περιπτώσεις η εφαρμογή πρέπει να γνωρίζει ποιο λειτουργικό σύστημα θέλουμε να κρυπτογραφήσουμε αν όχι όλα, κάνοντας και τις απαραίτητες ρυθμίσεις στον boot loader της.



Screenshot 17 Επιλογή αριθμού εγκατεστημένων λειτουργικών συστημάτων

Το δικό μας σύστημα έχει ένα λειτουργικό σύστημα εγκατεστημένο, οπότε κάνουμε την αντίστοιχη επιλογή και προχωράμε.

6.4.4 Επιλογές κρυπτογράφησης

4ο Βήμα: Σε αυτό το βήμα θα κάνουμε ίσως τις πιο σημαντικές επιλογές οι οποίες αφορούν την κρυπτογράφηση που θα εφαρμοστεί στον δίσκο:

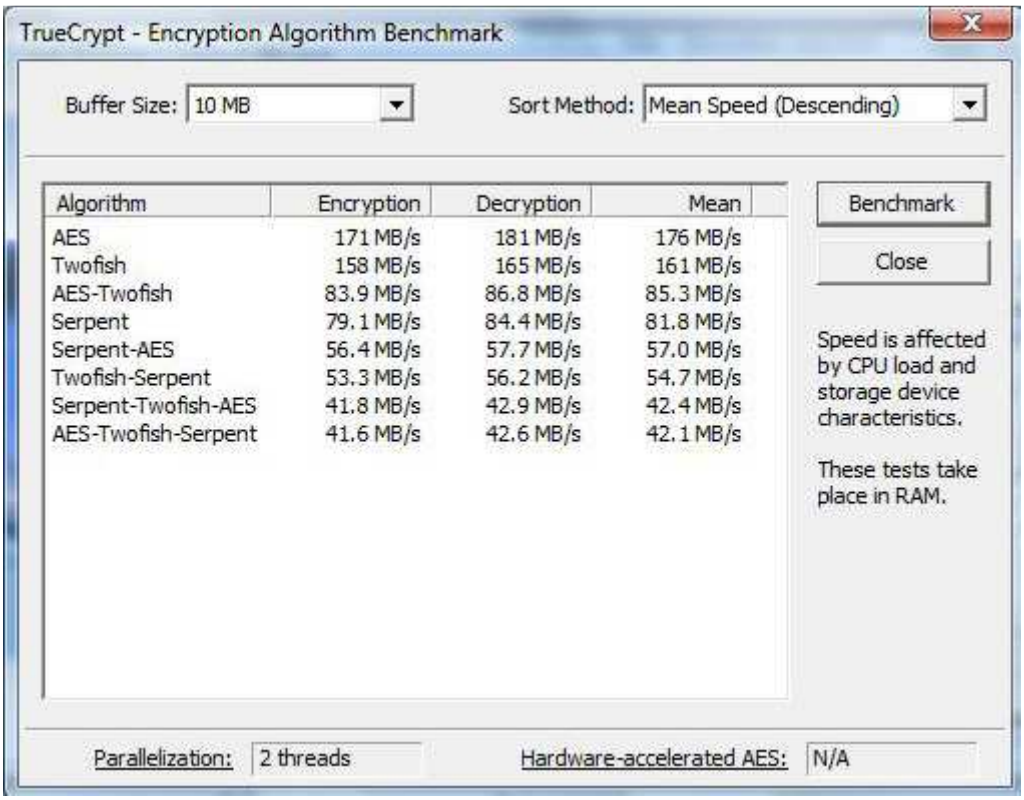
1. Επιλογή αλγόριθμου κρυπτογράφησης.
   Το TrueCrypt μας επιτρέπει να επιλέξουμε μεταξύ τριών αλγορίθμων κρυπτογράφησης συμμετρικού κλειδιού. Τους AES, Serpent και Twofish, αλλά και συνδυασμούς δύο ή τριών από αυτούς (Screenshot 18).

Screenshot 18 Επιλογή αλγορίθμου κρυπτογράφησης

Η επιλογή του χρήστη θα πρέπει να γίνει με ιδιαίτερη προσοχή και με βάση το επίπεδο ασφάλειας που επιθυμεί και την ταχύτητα εφαρμογής των αλγορίθμων σε πραγματικό χρόνο. Για να μας βοηθήσει σε αυτή την επιλογή το TrueCrypt διαθέτει ένα μετρητή επιδόσεων ο οποίος ανοίγει πατώντας το κουμπί “Benchmark” και μας παρουσιάζει μετρήσεις της ταχύτητας κρυπτογράφησης/αποκρυπτογράφησης του κάθε αλγόριθμου και των συνδυασμών τους για το σύστημα μας και σε σχέση με το μέγεθος του buffer (Screenshot 19). Οι μετρήσεις αυτές δείχνουν τον μέσο όγκο δεδομένων (σε Megabytes) που κρυπτογραφούνται και αποκρυπτογραφούνται από τον υπολογιστή ανά δευτερόλεπτο (MB/s).

Γενικά ισχύει πως ο συνδυασμός δύο ή περισσότερων αλγόριθμων προσφέρει υψηλότερα επίπεδα ασφάλειας, συνήθως όμως με σημαντικό κόστος στις επιδόσεις του υπολογιστή και στον αρχικό χρόνο εφαρμογής. Ενώ διαφορετικοί αλγόριθμοι και οι συνδυασμοί τους ανταποκρίνονται διαφορετικά και σε σχέση με το μέγεθος του buffer. Ο πιο γρήγορος αλγόριθμος είναι ο AES όταν χρησιμοποιείται μόνος του και στο δικό μας σύστημα απέδιδε περίπου 180 MB/s. Ο πιο αποδοτικός διπλός συνδυασμός είναι ο AES-Twofish με 85 MB/s ενώ ο Serpent-Twofish-AES είναι ο γρηγορότερος από τους τριπλούς με την μέση

ταχύτητα όμως να πέφτει κοντά στα 40 MB/s πολλαπλασιάζοντας ταυτόχρονα και τον αρχικό χρόνο εφαρμογής. Ο χρήστης καλείται να επιλέξει την ισορροπία ανάμεσα σε ασφάλεια και ταχύτητα. Σε αυτήν την πρακτική εφαρμογή επιλέξαμε απλό AES, αφού προσφέρει ικανοποιητικά επίπεδα ασφάλειας σε συνδυασμό με γρήγορη ανταπόκριση σε πραγματικό χρόνο και σχετικά χαμηλό αρχικό χρόνο εφαρμογής.



Screenshot 19 Μετρητής επιδόσεων αλγόριθμων κρυπτογράφησης

2. Επιλογή αλγόριθμου κατακερματισμού (hash) (Screenshot 20).

Οι αλγόριθμοι κατακερματισμού είναι μαθηματικές συναρτήσεις που δέχονται ως είσοδο ένα αυθαίρετο μέγεθος δεδομένων και δίνουν ως έξοδο μια σειρά στοιχείων (συμβολοσειρά) καθορισμένου αριθμού bit, τέτοια ώστε οποιαδήποτε αλλαγή γίνει σε αυτά τα δεδομένα, να επηρεάζει και το αποτέλεσμα στην συμβολοσειρά (32).

Το TrueCrypt μας επιτρέπει να επιλέξουμε μεταξύ των RIPEMD-160, SHA-512 και Whirlpool. Και οι τρείς αυτοί αλγόριθμοι κατακερματισμού χρησιμοποιούν περίπου την ίδια μεθοδολογία, με τη διαφορά ότι ο RIPEMD-160 δίνει στην έξοδο συμβολοσειρές με μέγεθος 160 bit ενώ οι SHA-512 και Whirlpool έχουν ως έξοδο, συμβολοσειρές των 512 bit και μπορούν να λάβουν στην είσοδο block δεδομένων έως και διπλάσιου μεγέθους.

Ο πιο διαδεδομένος από τους τρείς είναι ο SHA-512 ή αλλιώς SHA-2 και αποτελεί την επιλογή μας, ενώ υπό κατασκευή είναι και ο διάδοχος του ονόματι SHA-3 που αναμένεται κάποια στιγμή το 2012.

Screenshot 20 Επιλογή αλγορίθμου κατακερματισμού

6.4.5 Κωδικοί και κλειδιά κρυπτογράφησης

5ο Βήμα: Σε αυτό το βήμα πρέπει να ορίσουμε τον μυστικό κωδικό, με τη χρήση του οποίου θα μπορούμε να έχουμε πρόσβαση στα δεδομένα (Screenshot 21).

Ο μυστικός κωδικός είναι πολύ σημαντικός και ο χρήστης πρέπει να είναι πολύ προσεχτικός στην επιλογή του, λαμβάνοντας υπόψη κάποιες σημαντικές παραμέτρους ώστε να δημιουργήσει ένα ισχυρό κωδικό:

1. Ο κωδικός πρέπει να αντιστέκεται σε εικασίες και γενικά να είναι δύσκολο να τον μαντέψει κάποιος εισβολέας.
2. Προτείνεται ο κωδικός να μην αποτελείται από λέξεις ή συνδυασμό λέξεων που υπάρχουν σε γλωσσικά λεξικά.
3. Δεν προτείνεται η χρήση ονομάτων ή ημερομηνίας γέννησης.
4. Ένας καλός και ισχυρός κωδικός αποτελείται από ένα συνδυασμό τυχαίων χαρακτήρων (κεφαλαίων και μικρών), αριθμών και ειδικών συμβόλων (@#$%&*).
5. Ισχύει γενικά ο κανόνας: όσο μεγαλύτερο είναι το μήκος ενός κωδικού τόσο ισχυρότερος είναι.

Το TrueCrypt μας προτείνει ο κωδικός μας να έχει μήκος τουλάχιστον 20 χαρακτήρων και αναφέρει ότι το μέγιστο υποστηριζόμενο μήκος κωδικών είναι 64 χαρακτήρες. Σε περίπτωση που ο κωδικός είναι μικρός ή σχετικά ανίσχυρος η εφαρμογή μας εμφανίζει ένα μήνυμα προειδοποίησης, αλλά τελικά επιτρέπει την χρήση οποιουδήποτε κωδικού. Επίσης αν ο χρήστης επιθυμεί ένα επιπλέον έλεγχο ασφαλείας έχει τη δυνατότητα να συνδέσει τη χρήση του κωδικού με κρυπτογραφημένα αρχεία κλειδιά από μια συσκευή ασφαλείας.

Screenshot 21 Επιλογή μυστικού κωδικού

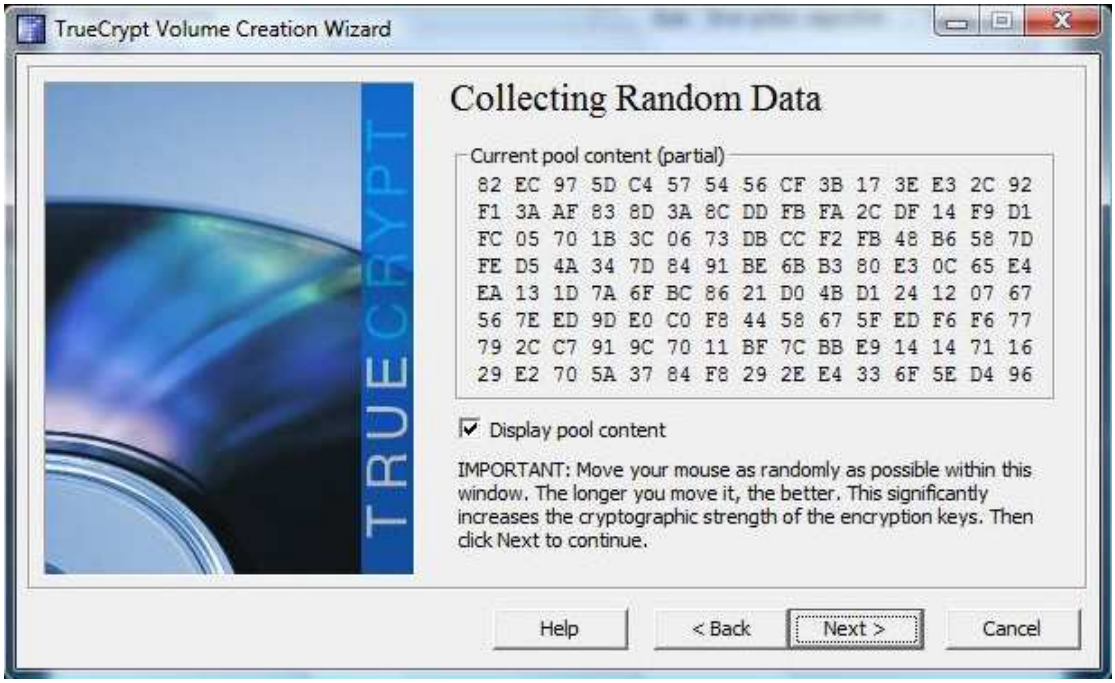
6ο Βήμα: Στο σημείο αυτό το TrueCrypt θα δημιουργήσει τα διάφορα κλειδιά που θα χρησιμοποιηθούν στην κρυπτογράφηση του συστήματος (κλειδί κεφαλής, κύριο κλειδί, δευτερεύον κλειδί, «αλάτι», αρχεία κλειδιά) μέσω μιας γεννήτριας τυχαίων αριθμών (Screenshot 22).

Για να αυξήσει την ποικιλία και την μοναδικότητα των παραγόμενων κλειδιών η γεννήτρια αυτή δημιουργεί ένα πίνακα τυχαίων τιμών 320 byte ο οποίος γεμίζει δεδομένα λαμβάνοντας υπόψη τους εξής παράγοντες:

1. Την κίνηση που διαγράφει το ποντίκι
2. Το πάτημα πλήκτρων του πληκτρολογίου
3. Δεδομένα από προγράμματα των Windows (CryptoAPI, NETAPI32) αλλά και διάφορους χειριστές, μεταβλητές χρόνου και μετρητές των Windows.

Η εφαρμογή λοιπόν καλεί τον χρήστη να κάνει τυχαίες κινήσεις με το ποντίκι και να πληκτρολογήσει τυχαίους χαρακτήρες για να ισχυροποιήσει την μοναδικότητα των κλειδιών που θα δημιουργηθούν από τον πίνακα τυχαίων τιμών σε συνδυασμό με τα δεδομένα που λαμβάνει από τα Windows. Τα περιεχόμενα της «λίμνης» τυχαίων τιμών παρουσιάζονται στο χρήστη σε πραγματικό χρόνο καθώς μεταβάλλονται από τους παράγοντες που προαναφέραμε.

7ο Βήμα: Πηγαίνοντας στο επόμενο βήμα, η εφαρμογή εμφανίζει το αρχικό κομμάτι των δύο σημαντικότερων κλειδιών που δημιουργήθηκαν (Screenshot 23), ενώ αν για κάποιο λόγο ο χρήστης δεν είναι ευχαριστημένος από το αποτέλεσμα μπορεί να γυρίσει ένα βήμα πίσω επαναλαμβάνοντας την διαδικασία και να δημιουργήσει καινούργια κλειδιά.



Screenshot 22 Λίμνη γεννήτριας τυχαίων αριθμών

Screenshot 23 Παραγόμενα κλειδιά

6.4.6 Δίσκος διάσωσης

8ο Βήμα: Πριν εκκινήσει την διαδικασία κρυπτογράφησης, το TrueCrypt απαιτεί από τον χρήστη να δημιουργήσει ένα δίσκο διάσωσης (Rescue Disk) (Screenshot 24). Αυτός ο δίσκος είναι αρχείο μορφής .iso και αποθηκεύεται σε ένα προορισμό επιλογής του χρήστη.

Ο χρήστης μετά καλείται να φορτώσει αυτό το αρχείο σε ένα πρόγραμμα εγγραφής CD/DVD και να το αποτυπώσει σε ένα δίσκο CD ή DVD, εμείς χρησιμοποιήσαμε για αυτό το σκοπό την εφαρμογή Nero Burning Rom.

Screenshot 24 Αποθήκευση δίσκου διάσωσης

9ο Βήμα: Στη συνέχεια το TruCrypt ελέγχει τον δίσκο διάσωσης που μόλις δημιούργησε ο χρήστης και αν επικυρωθεί επιτρέπει την μετάβαση στο επόμενο βήμα (Screenshot 25).

Screenshot 25 Επικύρωση δίσκου διάσωσης

Ο δίσκος διάσωσης μεταξύ άλλων σημαντικών πληροφοριών και δεδομένων εμπεριέχει και όλα τα κλειδιά κρυπτογράφησης που δημιουργήθηκαν στο βήμα 6. Σε οποιαδήποτε περίπτωση καταστροφής, κρίσιμου για την εφαρμογή λογισμικού (π.χ. boot loader), ο δίσκος διάσωσης δίνει την δυνατότητα επαναφοράς των κατεστραμμένων αρχείων της εφαρμογής. Σε περίπτωση καταστροφικού

προβλήματος στο λειτουργικό σύστημα, ο χρήστης έχει τη δυνατότητα να αποκρυπτογραφήσει όλα τα δεδομένα του σε συνδυασμό με τον σωστό μυστικό κωδικό.

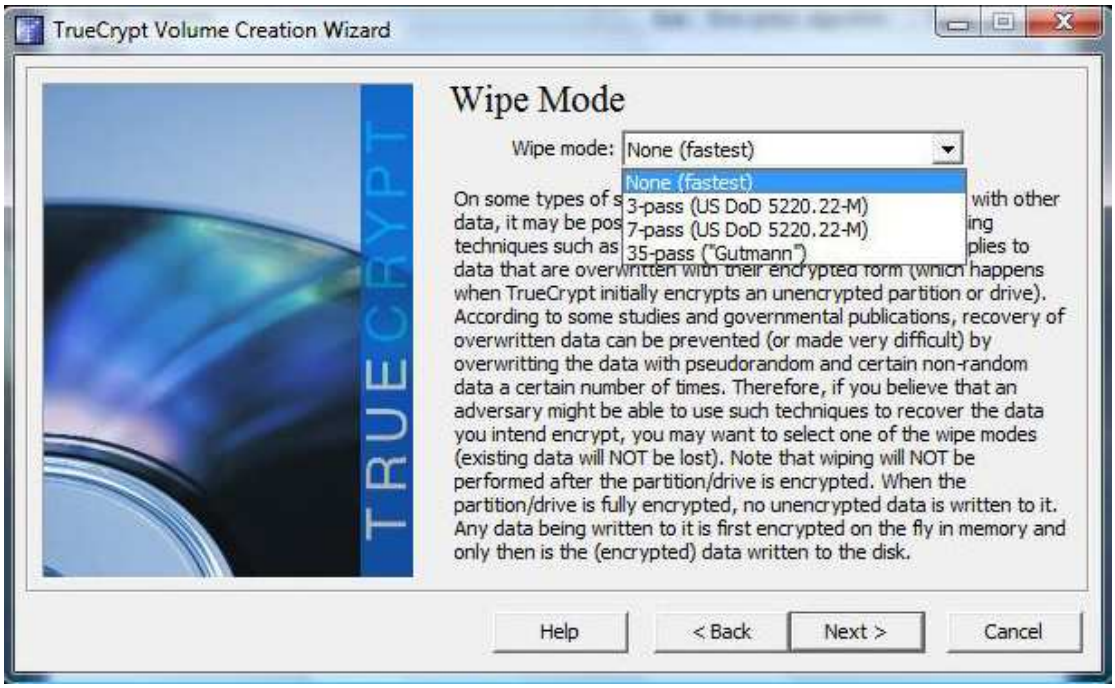
6.4.7 Wipe mode

Είναι δυνατό σε μαγνητικούς τύπους σκληρών δίσκων να χρησιμοποιηθεί μια μέθοδος μαγνητικής μικροσκοπίας κατά την οποία επαναφέρονται δεδομένα που έχουν καταργηθεί και αντικατασταθεί από νέα δεδομένα. Επειδή λοιπόν κατά την κρυπτογράφηση το TrueCrypt αντικαθιστά τα μη κρυπτογραφημένα δεδομένα με την κρυπτογραφημένη μορφή τους, τα καθιστά ευαίσθητα σε σαρώσεις μαγνητικής μικροσκοπίας.

Για να προστατέψει τα δεδομένα μας το TrueCrypt έχει την δυνατότητα να εφαρμόσει κάποιο αριθμό επαναλήψεων αντικατάστασης δεδομένων (χρησιμοποιώντας ένα συνδυασμό τυχαίων και μη δεδομένων) πριν κάνει την τελική εγγραφή των πραγματικών δεδομένων. Αυτή η διαδικασία ονομάζεται μέθοδος «κάθαρσης» (Wipe mode) και σύμφωνα με μελέτες εμποδίζει την ανάκτηση δεδομένων από μεθόδους μαγνητικής μικροσκοπίας.

10^{ο} Βήμα: Ως τελευταία επιλογή πριν την έναρξη κρυπτογράφησης ο χρήστης καλείται να επιλέξει τον αριθμό τον επαναλήψεων της μεθόδου «κάθαρσης» (Screenshot 26).

Πρέπει να σημειώσουμε εδώ ότι κάθε επανάληψη αυξάνει σημαντικά τον χρόνο της αρχικής κρυπτογράφησης του συστήματος, ενώ ο χρήστης μπορεί και να επιλέξει να την παραλείψει εντελώς.



Screenshot 26 Επιλογή επαναλήψεων Wipe mode

Πρακτικά δεν είναι απαραίτητη η εφαρμογή της διαδικασίας wipe παρά μόνο σε περίπτωση εξαιρετικά ευαίσθητων δεδομένων υψίστης ασφαλείας. Η μαγνητική μικροσκοπία είναι μια επίπονη και περίπλοκη διαδικασία με πρακτικά χαμηλή

αποτελεσματικότητα ενώ απαιτεί και την φυσική κατοχή του σκληρού δίσκου από τον επίδοξο υποκλοπέα.

6.4.8 Έναρξη και ολοκλήρωση διαδικασίας κρυπτογράφησης δίσκου

11ο Βήμα: Στο τελευταίο βήμα πριν την έναρξη της κρυπτογράφησης συστήματος το TrueCrypt μας ενημερώνει ότι θα κάνει μια δοκιμή για να επιβεβαιώσει ότι όλα τα υποσυστήματα του θα δουλέψουν σωστά και σύμφωνα με τις επιλογές μας (Screenshot 27).

Screenshot 27 Δοκιμή και επανεκκίνηση συστήματος

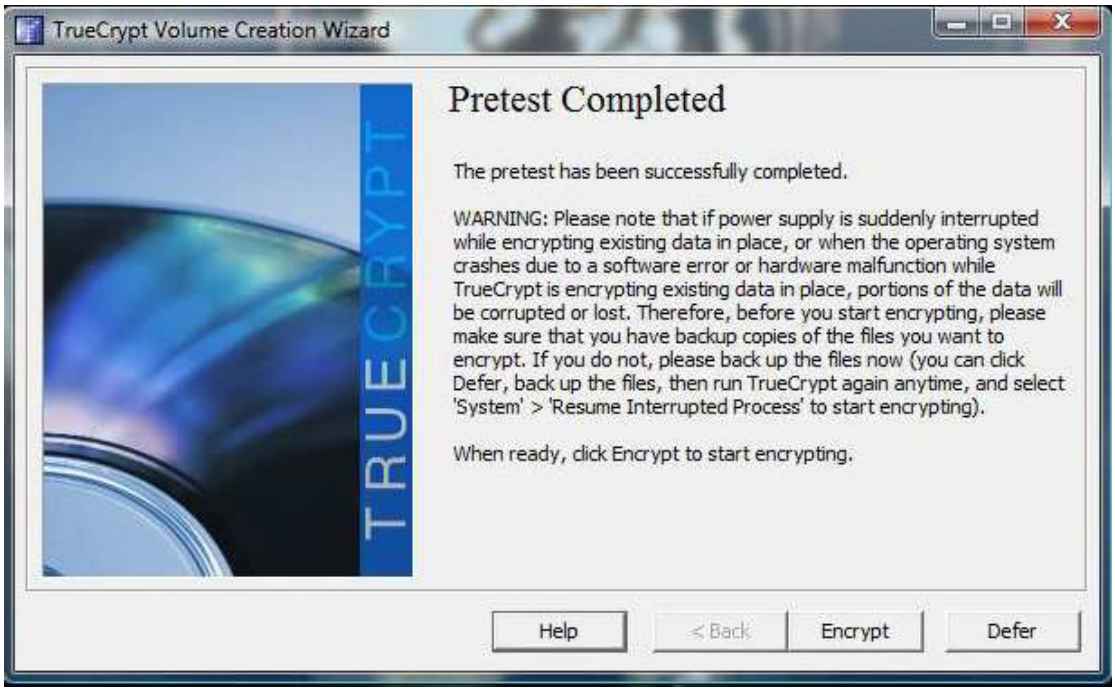
Όταν ο χρήστης πατήσει το κουμπί “Test” η εφαρμογή θα εγκαταστήσει όλα τα απαραίτητα υποσυστήματα της (το boot loader κ.α.) και θα κάνει επανεκκίνηση του υπολογιστή. Κατά την εκκίνηση και πριν φορτωθούν τα Windows ,το TrueCrypt Boot Loader θα τρέξει για πρώτη φόρα και ο χρήστης θα πρέπει να εισάγει τον μυστικό του κωδικό.

12ο Βήμα: Μετά την επανεκκίνηση και μόλις φορτωθούν τα Windows η εφαρμογή κρυπτογράφησης του TrueCrypt θα ανοίξει αυτόματα ενημερώνοντας τον χρήστη για τα αποτελέσματα τις δοκιμής, αναφέροντας παράλληλα και μερικές προειδοποιήσεις (Screenshot 28).

Σε περίπτωση απρόσμενης διακοπής της παροχής ρεύματος ή κατάρρευσης του υπολογιστή λόγο κάποιου υλικού ή λογισμικού προβλήματος και ενώ το TrueCrypt κρυπτογραφεί τα υπάρχοντα δεδομένα, υπάρχει περίπτωση ένα μέρος αυτών των δεδομένων να διαβρωθεί ή να χαθεί. Για αυτό το λόγο προτείνει στον χρήστη πριν ξεκινήσει την διαδικασία κρυπτογράφησης να διαθέτει αντίγραφο ασφαλείας (back-up) όλων των αρχείων που θα κρυπτογραφηθούν.

Όταν κρυπτογραφούμε μεγάλους δίσκους γεμάτους δεδομένα, είναι πρακτικά αδύνατο να πάρουμε αντίγραφο ασφαλείας όλων των δεδομένων. Σε τέτοια περίπτωση ο χρήστης μπορεί να κάνει αντίγραφα ασφαλείας μόνο για κρίσιμα και

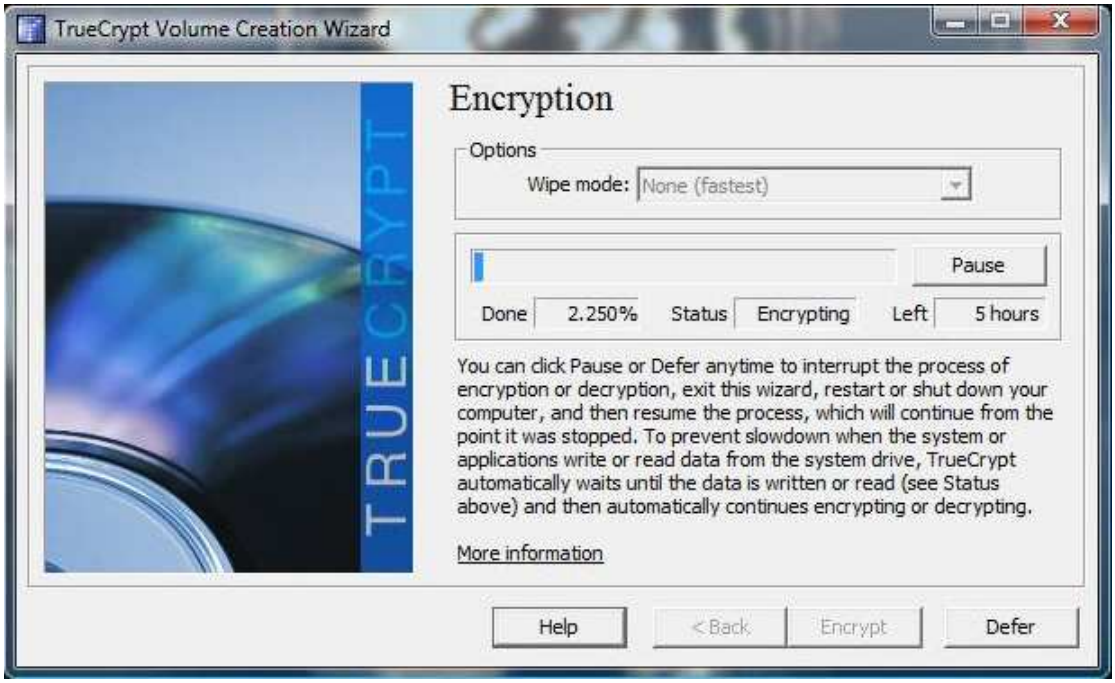
αναντικατάστατα δεδομένα του. Επίσης προτείνεται η χρήση UPS (σταθεροποιητή ρεύματος) συνδεμένου με τον υπολογιστή, μειώνοντας με αυτό τον τρόπο σημαντικά τις πιθανότητες εμφάνισης κάποιου προβλήματος και κατά συνέπεια, απώλειας δεδομένων.



Screenshot 28 Εκκίνηση διαδικασίας κρυπτογράφησης συστήματος

Τέλος αν η δοκιμή ήταν επιτυχής ο χρήστης μπορεί να ξεκινήσει άμεσα την διαδικασία κρυπτογράφησης πατώντας το κουμπί “Encrypt”.

13ο Βήμα: Όταν ο χρήστης εκκινήσει την διαδικασία κρυπτογράφησης δεν έχει παρά να περιμένει την ολοκλήρωση της, η οποία μπορεί να διαρκέσει αρκετές ώρες. Η εφαρμογή παρέχει ως επιπλέον πληροφορία και μια εκτίμηση του χρόνου που απομένει, ενώ ο χρήστης διατηρεί την δυνατότητα να διακόψει και να συνεχίσει την διαδικασία όποτε ο ίδιος επιθυμεί χωρίς καμία επίπτωση (Screenshot 29).



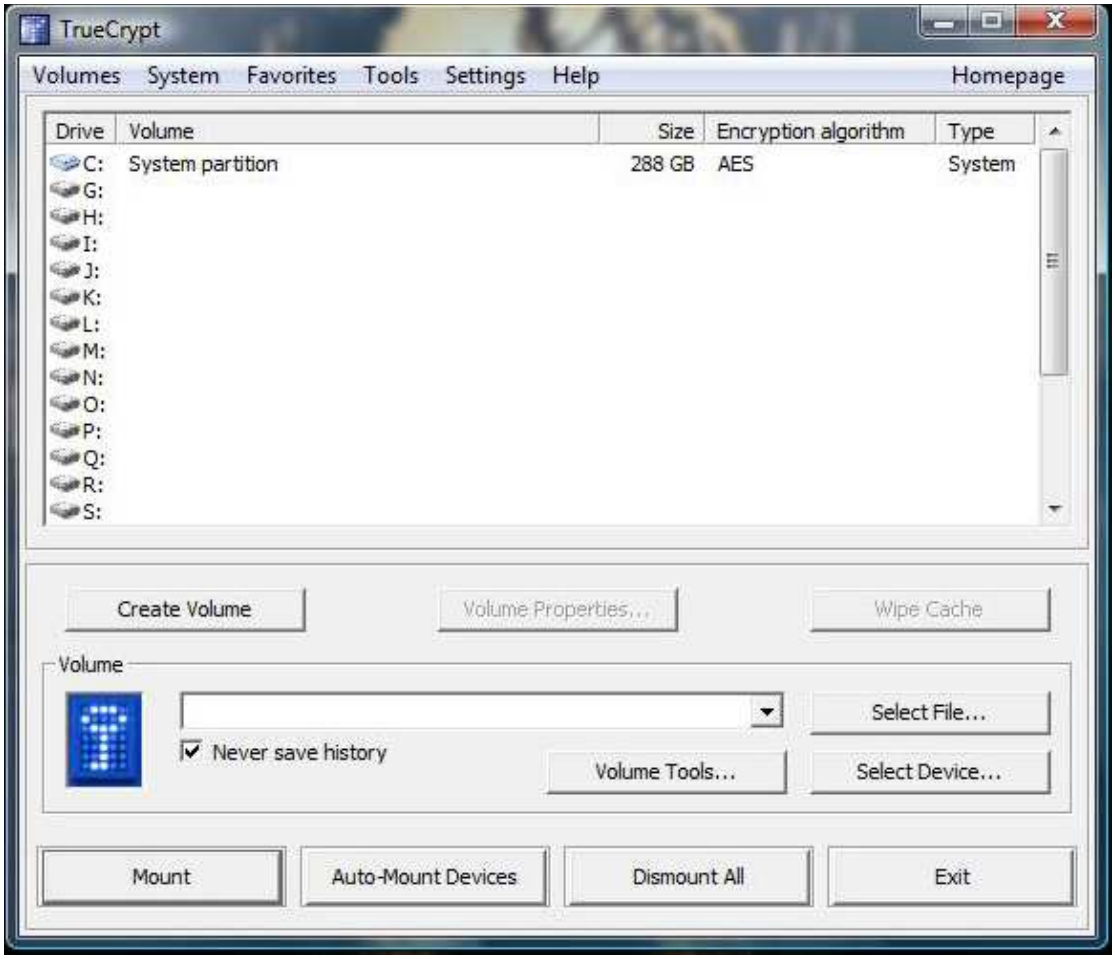
Screenshot 29 Κρυπτογράφηση δεδομένων εν λειτουργία

Ο χρόνος που χρειάζεται η διαδικασία κρυπτογράφησης διαφέρει από περίπτωση σε περίπτωση και εξαρτάται από πολλούς παράγοντες. Μεταξύ αυτών: το υλικό που διαθέτει ο προσωπικός υπολογιστής, τον όγκο των δεδομένων που θα κρυπτογραφηθούν, τον συνδυασμό αλγορίθμων και τις επαναλήψεις της διαδικασίας Wipe που επιλέξαμε.

14^{ο} Βήμα: Η διαδικασία ολοκληρώθηκε (Screenshot 30).

Screenshot 30 Ολοκλήρωση κρυπτογράφησης

Ο τόμος του λειτουργικού συστήματος με όλα τα δεδομένα που περιέχει είναι πλέον κρυπτογραφημένος με αλγόριθμο AES (Screenshot 31). Η εφαρμογή του TrueCrypt θα εκτελείται αυτόματα κατά την εκκίνηση των Windows και θα είναι πάντα ενεργή. Από αυτό το σημείο και πέρα όλα τα δεδομένα θα κρυπτογραφούνται με AES πριν αποθηκευθούν στον συγκεκριμένο τόμο, ενώ τα δεδομένα που μεταφέρονται από αυτόν σε άλλους μη κρυπτογραφημένους δίσκους, θα αποκρυπτογραφούνται πριν την μεταφορά.



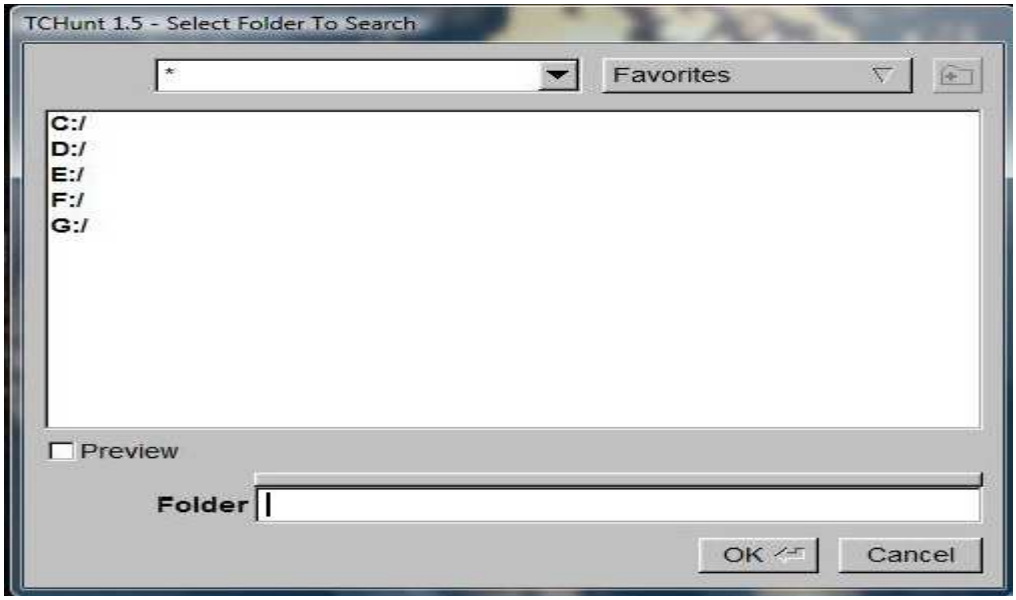
Screenshot 31 Κυρίως μενού TrueCrypt

6.5 Αδυναμίες ασφαλείας TrueCrypt

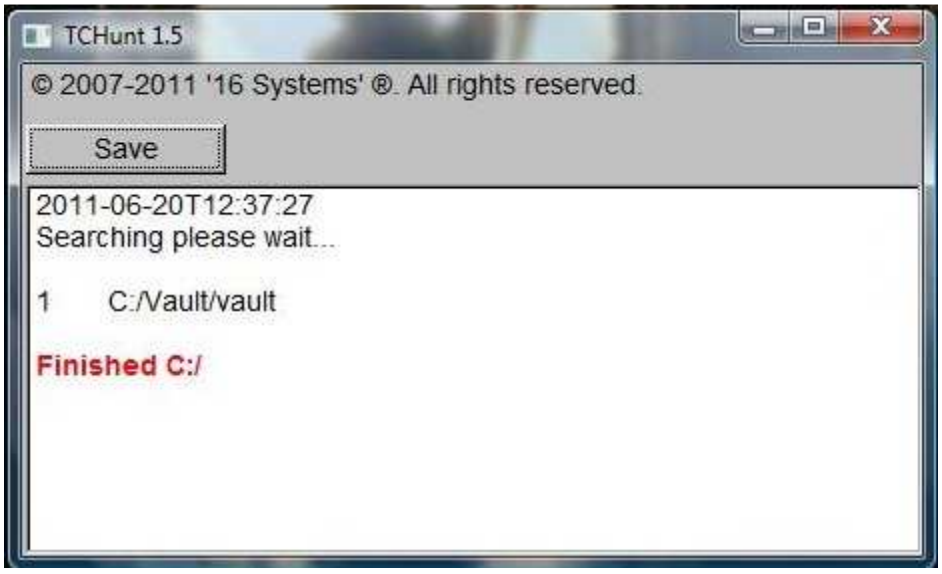
Χρησιμοποιώντας το TrueCrypt, η ασφάλεια των κρυπτογραφημένων δεδομένων βασίζεται στην μυστικότητα του κωδικού κρυπτογράφησης. Αν κάποιος υποκλοπέας λάβει με οποιονδήποτε τρόπο γνώση του μυστικού κωδικού, αυτόματα αποκτά πρόσβαση σε όλα τα δεδομένα του χρήστη. Μια λύση σε αυτό το πρόβλημα δίνεται με τη δημιουργία ενός κρυφού τόμου, μέσα σε έναν ήδη κρυπτογραφημένο τόμο, χρησιμοποιώντας διαφορετικό αλγόριθμο κρυπτογράφησης και μυστικό κωδικό.

Ακόμα και με τη χρήση κρυφών τόμων όμως, ένας εισβολέας με χρήση κατάλληλου λογισμικού σάρωσης δεδομένων μπορεί τελικά να ανακαλύψει την

ύπαρξη κρυφών τόμων. Ένα τέτοιο λογισμικό ελεύθερο προς χρήση είναι το TCHunt (33) το οποίο έχει την δυνατότητα να σαρώνει επιλεγμένες περιοχές και να επισημαίνει πιθανούς κρυπτογραφημένους τόμους (Screenshot 32,33).



Screenshot 32 Κυρίως Μενού TCHunt



Screenshot 33 Σάρωση TCHunt

Σε περίπτωση που ο υπολογιστής του χρήστη εμπεριείχε κακόβουλο λογισμικό πριν την κρυπτογράφηση των δεδομένων ή προσβληθεί από κακόβουλο λογισμικό σε περιοχή του δίσκου που δεν είναι κρυπτογραφημένη, υπάρχει δυνατότητα υποκλοπής των κωδικών από ένα πιθανό χειριστή τέτοιου είδους λογισμικού, ο οποίος θα μπορούσε να λαμβάνει πληροφορίες που εκπέμπονται προς αυτόν από το κακόβουλο λογισμικό. Ένα πρόσφατο παράδειγμα λογισμικού, που εκμεταλλεύεται μια αδυναμία του λειτουργικού συστήματος, αναφέρεται στο ηλεκτρονικό άρθρο «BitLocker / TrueCrypt Vulnerability» (34).

Παρόμοια, αν ένας υποκλοπέας έχει φυσική πρόσβαση στον υπολογιστή του χρήστη θα μπορούσε να συνδέσει ένα keylogger (υλικό καταγραφής

πληκτρολόγησης) ή μια συσκευή καταγραφής μνήμης, λαμβάνοντας έτσι γνώση των κωδικών ή/και των κλειδιών κρυπτογράφησης.

Όπως έχουμε προαναφέρει, το TrueCrypt εφαρμόζει την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων σε πραγματικό χρόνο στην μνήμη του υπολογιστή. Αν λοιπόν ένας εισβολέας καταφέρει να πάρει ένα αντίγραφο της μνήμης του συστήματος, μπορεί να αναλύσει τις πληροφορίες που εμπεριείχε η μνήμη και κατά συνέπεια να αποκαλύψει τον μυστικό κωδικό ή/και τα κλειδιά κρυπτογράφησης. Υπάρχουν πολλές εφαρμογές καταγραφής μνήμης, μια από αυτές είναι το ελεύθερο λογισμικό MDD (35) (Screenshot 34). Στην συνέχεια και με χρήση κατάλληλου λογισμικού ανάγνωσης δεδομένων μνήμης, όπως το MANDIANT Audit Viewer (36), μπορεί να γίνει ανάλυση των δεδομένων που βρίσκονταν στην μνήμη του συστήματος και να εντοπιστούν κωδικοί, κλειδιά και γενικά κρίσιμες πληροφορίες του συστήματος.

Screenshot 34 Καταγραφή και αποθήκευση μνήμης στο αρχείο memorydump.dd

Πρέπει να σημειώσουμε εδώ, ότι η μνήμη ενός υπολογιστή περιέχει πολλές και διάφορες πληροφορίες και δεδομένα που μπορούν να έχουν συνολικό μέγεθος έως και μερικά gigabyte, ιδιαίτερα σε σύγχρονα συστήματα. Για το λόγο αυτό ο εντοπισμός ενός κωδικού ή κλειδιού μέσα σε ένα τόσο μεγάλο όγκο δεδομένων είναι μια περίπλοκη και επίπονη διαδικασία με μέτρια αποτελεσματικότητα. Σε περίπτωση όμως που ο επίδοξος υποκλοπέας γνωρίζει ή μπορεί να αναγνωρίσει τον αλγόριθμο με τον οποίο κρυπτογραφήθηκε το σύστημα, έχει πολύ περισσότερες πιθανότητες να ανακαλύψει τους κωδικούς, περιορίζοντας την αναζήτηση του σε δεδομένα που έχουν χαρακτηριστικά παρόμοια με αυτά των κλειδιών του αλγόριθμου.

Τέλος όπως αναφέραμε στο κεφάλαιο 5, όλες οι εφαρμογές πλήρους κρυπτογράφησης δίσκου αδυνατούν να κρυπτογραφήσουν το πεδίο MBR του σκληρού δίσκου, έτσι ένας εισβολέας με χρήση κατάλληλου λογισμικού MBR rootkit, όπως το Stoned Bootkit (37), μπορεί να παρακάμψει την κρυπτογράφηση του δίσκου. Το ηλεκτρονικό άρθρο «Bootkit bypasses hard disk encryption», αναφέρεται αναλυτικά στην λειτουργία του Stoned Bootkit.

6.6 Συμπεράσματα και προτάσεις

Στην πτυχιακή αυτή και με την πάροδο των κεφαλαίων, εξετάσαμε διαφορετικά επίπεδα ασφάλειας και τις εφαρμογές ή το υλικό μέσω του οποίου υλοποιούνται. Οι υλοποιήσεις αυτές, όπως είδαμε, διαφέρουν μεταξύ τους σε σχέση με το βαθμό ασφάλειας, το κόστος, την απόδοση και την ευκολία χρήσης που προσφέρουν.

Όλες οι υλοποιήσεις ασφαλείας είναι πιθανό να είναι ευάλωτες σε κάποιο είδος επιθέσεων ή με την πάροδο του χρόνου να παρουσιάσουν κάποια κενά ασφαλείας. Για αυτό το λόγο και για να επιτύχουμε υψηλά επίπεδα ασφάλειας σε ένα προσωπικό υπολογιστή, είναι σημαντικό να συνδυάσουμε εφαρμογές και υλικό ασφαλείας, που δρα σε διαφορετικά επίπεδα. Με αυτόν τον τρόπο ακόμα και αν κάποιος εισβολέας καταφέρει να περάσει ένα επίπεδο ελέγχου θα βρεθεί αντιμέτωπος με ένα άλλο εντελώς διαφορετικό.

Ένας καλός συνδυασμός λογισμικού και υλικού ασφαλείας με χαμηλό κόστος επιτυγχάνεται με χρήση λογισμικού πλήρους κρυπτογράφησης δίσκου, αντιϊκού λογισμικού και μιας συσκευής ασφαλείας.

Π.χ. Στο σύστημα μας, που εφαρμόσαμε την πλήρη κρυπτογράφηση και περιγράψαμε στο 6.3 χρησιμοποιήσαμε: ως αντιϊκό λογισμικό το Eset Smart Security (38), ως λογισμικό πλήρους κρυπτογράφησης δίσκου το TrueCrypt και ως συσκευή ασφαλείας τον ενσωματωμένο βιομετρικό σαρωτή δακτυλικού αποτυπώματος που διαθέτει το laptop.

Το TrueCrypt υποστηρίζει συνεργασία με οποιαδήποτε συσκευή ασφαλείας υλοποιεί το πρωτόκολλο PKCS#11 αλλά και νεότερες εκδόσεις του. Παρακάτω αναφέρουμε ενδεικτικά μερικές συσκευές ασφαλείας που μπορεί ο χρήστης να συνδυάσει με το TrueCrypt και το αντίστοιχο κόστος τους:

- ASEKey Crypto USB Token (39): συσκευή ασφαλείας USB με ενσωματωμένους αλγόριθμους RSA 2048, 3DES, DES, AES και κόστος 55 ευρώ.
- ePass1000 USB (40): συσκευή ασφαλείας USB με ενσωματωμένους αλγόριθμους RSA 1024-bit / 2048-bit, DES, 3DES, SHA1 και κόστος 25 ευρώ.
- IDProtect Smart Card (41) και ASEDrive IIIe USB V2 Smart Card Reader (42): Έξυπνη κάρτα με υποστηριζόμενη κρυπτογραφία RSA 2048, 3DES, DES, AES, SHA-1, SHA-256 και κόστος 25 ευρώ. Συσκευή ανάγνωσης έξυπνων καρτών κόστους 27 ευρώ.
- Eikon Digital Privacy Manager - USB fingerprint reader (43): βιομετρικός σαρωτής δακτυλικού αποτυπώματος από την εταιρία Upek. Υποστηρίζει λειτουργικά συστήματα Windows, Mac και Unix και έχει κόστος 30 ευρώ. (Αυτή η συσκευή συνεργάζεται με το λειτουργικό σύστημα του χρήστη και όχι με το TrueCrypt)

Βιβλιογραφία

1. **Microsoft.** Windows. *Microsoft.* [Online] http://windows.microsoft.com/.

2. —. Windows Firewall . *Microsoft TechNet.* [Online] Microsoft Corporation, 2011. http://technet.microsoft.com/en-us/network/bb545423.

3. —. Windows Defender. *Microsoft.* [Online] http://www.microsoft.com/windows/products/winfamily/defender/.

4. **Βικιπαίδεια.** Ιός (υπολογιστές). *Βικιπαίδεια.* [Ηλεκτρονικό] 2011. http://el.wikipedia.org/wiki/Ιός_υπολογιστές.

5. —. Κρυπτογραφία. *Βικιπαίδεια.* [Ηλεκτρονικό] 2011. http://el.wikipedia.org/wiki/Κρυπτογραφία.

6. **Wikipedia.** Advanced Encryption Standard. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

7. **TrueCrypt.** Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux. *TrueCrypt.* [Online] http://www.truecrypt.org/.

8. **Wikipedia.** PGP Corporation. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/PGP_Corporation.

9. **Wikipedia.** Steganography. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Steganography.

10. —. Huffman coding. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Huffman_encoding.

11. **Nakasoft.** Xiao Steganography. *Cnet Downloads.* [Online] http://download.cnet.com/Xiao-Steganography/3000-2092_4-10541494.html.

12. **Wikipedia.** Security token. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Security_token.

13. —. One-time password. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/One-time_password.

14. **OUT-LAW.COM.** Phishing attack targets one-time passwords. *TheRegister.co.uk.* [Online] http://www.theregister.co.uk/2005/10/12/outlaw_phishing/.

15. **Wikipedia.** Two-factor authentication. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Two-factor_authentication.

16. **Finextra.** RSA hacked: SecurID two factor authentication data leaked. *Finextra.com.* [Online] http://www.finextra.com/news/fullstory.aspx?newsitemid=22375.

17. **Wikipedia.** Fingerprint recognition. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Fingerprint_recognition.

18. **Antti Stén, Antti Kaseva, Teemupekka Virtanen.** Fooling Fingerprint Scanners - Biometric Vulnerabilities of the Precise Biometrics 100 SC Scanner. [Online] http://stdot.com/pub/ffs_article_asten_akaseva.pdf.

19. **Wikipedia.** Iris recognition. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Iris_recognition.

20. **Michael J.S. Kang, Oscar T. Plag.** Analysis of Vulnerabilities of Iris Scanning Personal Authentication. [Online] http://courses.ece.ubc.ca/412/previous_years/2007_1_spring/modules/term_project/reports/2007/vulnerabilities_of_iris_scanning.pdf.

21. **Vijayan, Jaikumar.** Laptop face-recognition tech easy to hack, warns Black Hat researcher. *ComputerWorld.com.* [Online] http://www.computerworld.com/s/article/9128264/Laptop_face_recognition_tech_easy_to_hack_warns_Black_Hat_researcher.

22. **Wikipedia.** Facial recognition system. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Facial_recognition_system.

23. —. Disk encryption. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Disk_encryption.

24. —. Hardware-based full disk encryption. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Hardware-based_full_disk_encryption.

25. —. Trusted Platform Module. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Trusted_Platform_Module.

26. **TCG.** *Trusted Computing Group.* [Online] http://www.trustedcomputinggroup.org/.

27. **Wikipedia.** Trusted Computing Group. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Trusted_Computing_Group.

28. **Microsoft.** BitLocker Drive Encryption. *Microsoft Windows.* [Online] http://windows.microsoft.com/en-US/windows7/products/features/bitlocker.

29. **CenterTools.** DriveLock. *CenterTools DriveLock.* [Online] http://www.drivelock.com/.

30. **McAfee.** McAfee Endpoint Encryption. *McAfee.* [Online] http://www.mcafee.com/us/products/endpoint-encryption.aspx.

31. **Symantec.** PGP Whole Disk Encryption. *Symantec.* [Online] http://www.symantec.com/business/whole-disk-encryption.

32. **Wikipedia.** Cryptographic hash function. *Wikipedia.* [Online] 2011. http://en.wikipedia.org/wiki/Cryptographic_hash_function.

33. **Systems, 16.** TCHunt. *16 Systems.* [Online] http://16s.us/TCHunt/.

34. **WiredPig.** BitLocker / TrueCrypt Vulnerability. *http://pgp.wiredpig.us/.* [Online] http://pgp.wiredpig.us/2010/bitlocker-truecrypt-vulnerability/.

35. **benstotts.** MDD. *MDD.* [Online] http://sourceforge.net/projects/mdd/.

36. **MANDIANT.** MANDIANT Audit Viewer. *MANDIANT.* [Online] http://www.mandiant.com/products/free_software/mandiant_audit_viewer/download.

37. **Kleissner, Peter.** Stoned Bootkit. *Stoned Bootkit.* [Online] http://www.stoned-vienna.com/.

38. **ESET.** ESET - Antivirus Software with Spyware and Malware Protection. *ESET.* [Online] http://www.eset.com/.

39. **Athena Smartcard Solutions.** ASEKey Crypto USB Token. *Athena Smartcard Solutions.* [Online] http://www.athena-scs.com/product.asp?pid=34.

40. **Feitain.** ePass1000 USB Key. *Feitain.* [Online] http://www.ftsafe.com/products/epass1000.html.

41. **Athena Smartcard Solutions.** IDProtect Smart Card. *Athena Smartcard Solutions.* [Online] http://www.athena-scs.com/product.asp?pid=22.

42. —. ASEDrive IIIe USB V2 Smart Card Reader. *Athena Smartcard Solutions.* [Online] http://www.athena-scs.com/product.asp?pid=1.

43. **Upek.** Eikon Solutions. *Upek.* [Online] http://www.upek.com/solutions/eikon/default.asp.

44. **Walker-Morgan, Dj.** Bootkit bypasses hard disk encryption. *H-online.com.* [Online] http://www.h-online.com/security/news/item/Bootkit-bypasses-hard-disk-encryption-742721.html.

Παράρτημα Α Ακρωνύμια - Συντομογραφίες

0-9	**2FA**	Two Factor Authentication
	3DES	Triple Data Encryption Standard
A	**AES**	Advanced Encryption Standard
B	**BBS**	Bulletin Board System
	BIOS	Basic Input/ Output System
	BIT	Binary Digit
C		
D	**DES**	Data Encryption Standard
	DRM	Digital Rights Management
E		
F	**FDE**	Full Disk Encryption
G	**GnuPG**	GNU Privacy Guard
H	**HCO**	Hybrid Cryptographic Optimizer
I	**ICF**	Internet Connection Firewall
	IDEA	International Data Encryption Algorithm
	IP	Internet Protocol
J		
K		
L		
M		
N		

O	**OS**	Operating System
	OTP	One Time Password
P	**PC**	Personal Computer
	PGP	Pretty Good Privacy
	PKCS	Public-Key Cryptography Standards
Q		
R	**RSA**	Rivest, Shamir and Adleman
S	**SED**	Self-Encrypting Drives
	SSC	Security Subsystem Class
	SWG	Storage Work Group
T	**TCG**	Trusted Computing Group
	TNC	Trusted Network Connect
	TPM	Trusted Platform Module
U	**UAC**	User Account Control
	UPS	Uninterruptible Power Supply
	USB	Universal Serial Bus
V		
W		
X		
Y		
Z		

Παράρτημα Β Παρουσίαση

Slide 1:

Παρουσίαση Πτυχιακής Εργασίας

Προστασία δεδομένων σε προσωπικούς υπολογιστές

Μουντοκαλάκης Μιχάλης

Slide 2:

Προστασία δεδομένων σε προσωπικούς υπολογιστές

Στόχοι Πτυχιακής:

- Να παρουσιάσουμε και εξηγήσουμε την προστασία που προσφέρει το λειτουργικό σύστημα των Windows.
- Να παρουσιάσουμε και εξηγήσουμε τις βασικές μεθόδους κρυπτογράφησης δεδομένων.
- Να εξηγήσουμε τα είδη και την χρησιμότητα των συσκευών ασφαλείας για προσωπικούς υπολογιστές.
- Να αναλύσουμε την έννοια και τις υλοποιήσεις, της πλήρους κρυπτογράφησης σκληρού δίσκου.
- Τέλος να εφαρμόσουμε πρακτικά ένα παράδειγμα πλήρους κρυπτογράφησης σκληρού δίσκου, να το αναλύσουμε και να παρουσιάσουμε μερικές αδυναμίες του.

Slide 3:

Θωράκιση λειτουργικού συστήματος

Συστήματα ασφάλειας ενσωματωμένα στο λειτουργικό σύστημα

- **Windows Firewall:** Τείχος προστασίας δικτύου.
- **Windows Defender:** Πρόγραμμα καταπολέμησης κακόβουλου λογισμικού.
- **Έλεγχος λογαριασμού χρήστη:** περιορίζει τα δικαιώματα όλων των εφαρμογών.
- **Κέντρο ασφαλείας:** Εμφανίζει σημαντικές πληροφορίες για την κατάσταση ασφάλειας του pc.
- **Κέντρο αντιγράφων ασφαλείας και επαναφοράς:** Δημιουργεί αντίγραφα ασφαλείας και επαναφέρει τον υπολογιστή σε προ-αποθηκευμένες καταστάσεις.
- **Κρυπτογράφηση μονάδων δίσκου BitLocker:** Λογισμικό πλήρους κρυπτογράφησης δίσκου διαθέσιμο μόνο στις εκδόσεις Business και Ultimate των Windows

Slide 4:

Θωράκιση λειτουργικού συστήματος

Επιπλέον προστασία - Απλές μέθοδοι προστασίας συστήματος

- Ιδιαίτερα σημαντική η εγκατάσταση επιπλέον αντιϊκού λογισμικού (π.χ. Norton, Eset, Avast, AVG).
- Συνεχής και άμεση αναβάθμιση του λειτουργικού συστήματος, των υποσυστημάτων του, αλλά και του αντιϊκού λογισμικού.
- Το Windows Firewall και γενικά όλα τα συστήματα ασφαλείας πρέπει να είναι πάντοτε ενεργοποιημένα.
- Ορισμός προγραμματισμένων εργασιών ανά τακτά χρονικά διαστήματα, σε όλες της εφαρμογές ασφαλείας που υποστηρίζουν αυτή την δυνατότητα (π.χ. Windows Defender, κέντρο αντιγράφων ασφαλείας και επαναφοράς, αντιϊκό λογισμικό).

Slide 5:

Κρυπτογράφηση δεδομένων

Κρυπτογραφώντας δεδομένα που θεωρούνται εμπιστευτικά τους προσδίδουμε ακόμα ένα επίπεδο ασφάλειας.

Η κρυπτογράφηση και αποκρυπτογράφηση δεδομένων γίνεται με τη χρήση ενός αλγόριθμου κρυπτογράφησης και ενός κλειδιού κρυπτογράφησης.

Η κρυπτογράφηση δεδομένων χωρίζεται σε τρείς βασικές κατηγορίες ανάλογα με την τεχνική κρυπτογράφησης που εφαρμόζει:

- **Κρυπτογράφηση συμμετρικού κλειδιού:** χρησιμοποιεί ένα κοινό κλειδί κατά την διαδικασία της κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στην μυστικότητα του κλειδιού αυτού. Διαδεδομένοι αλγόριθμοι κρυπτογράφησης συμμετρικού κλειδιού: AES, Blowfish, 3DES, Serpent, Twofish.

Slide 6:

Κρυπτογράφηση δεδομένων

- **Κρυπτογράφηση δημοσίου κλειδιού:** έχει δυο είδη κλειδιών ένα δημόσιο που χρησιμοποιείται για την κρυπτογράφηση και ένα ιδιωτικό για την αποκρυπτογράφηση. Το μήνυμα που κρυπτογραφείται με το δημόσιο κλειδί δεν μπορεί να αποκρυπτογραφηθεί παρά μόνο με τη χρήση του ιδιωτικού κλειδιού που είναι συνδεμένο με αυτό. Η πιο διαδεδομένη εφαρμογή κρυπτογράφησης δημοσίου κλειδιού είναι το PGP.
- **Ψηφιακή στεγανογραφία:** χρησιμοποιείται για απόκρυψη δεδομένων μέσα σε άλλα δεδομένα που δεν προδίδουν το περιεχόμενο τους όπως αρχεία εικόνας, ήχου ή εκτελέσιμα.
  - Η πιο διαδεδομένη χρήση της ψηφιακής στεγανογραφίας είναι η απόκρυψη κειμένου σε εικόνες, το κείμενο συμπιέζεται συνήθως με κωδικοποίηση Huffman, κρυπτογραφείται με συμμετρικό κλειδί για περισσότερη ασφάλεια και τέλος ενσωματώνεται στην εικόνα.

Slide 7:

Συσκευές ασφαλείας

Συσκευές κωδικού μιας χρήσης (OTP Tokens)

Προσθέτουμε ένα επιπλέον επίπεδο ασφαλείας με τη χρήση περιφερειακών συσκευών ασφαλείας (security tokens), οι οποίες απαιτούν την πιστοποίηση του χρήστη πριν από οποιαδήποτε ενέργεια. Η πιστοποίηση αυτή γίνεται μέσω χρήσης ή ακόμα και απλής κατοχής αυτών των φυσικών συσκευών.

- **Συσκευές κωδικού μιας χρήσης (OTP Tokens):** Οι κωδικοί μιας χρήσης είναι έγκυροι μόνο για μια πιστοποίηση/εξουσιοδότηση χρήστη. Παρέχουν κωδικούς βάσει χρόνου ή βάσει ενός μαθηματικού αλγορίθμου. Ακόμα και η υποκλοπή ενός τέτοιου κωδικού δεν δημιουργεί πρόβλημα ασφάλειας, καθώς ο κωδικός αυτός δεν θα είναι έγκυρος στην επόμενη πιστοποίηση.

Slide 8:

Συσκευές ασφαλείας

Πιστοποίηση διπλού παράγοντα (2FA)

- **Πιστοποίηση διπλού παράγοντα (2FA):** η εξουσιοδότηση απαιτεί δύο διαφορετικά είδη «αποδεικτικών στοιχείων». Το ένα αποδεικτικό στοιχείο είναι κάτι που ο χρήστης γνωρίζει (μυστικός κωδικός), και το δεύτερο κάτι που έχει στην κατοχή του (συσκευή ασφαλείας). Ανάλογα με το είδος τις συσκευής που παρέχει το δεύτερο κλειδί έχουμε τις εξής κατηγορίες:
  - Συσκευές ασφαλείας USB (USB Tokens)
  - Έξυπνες κάρτες (Smart Cards)
  - Ασύρματες συσκευές ασφαλείας (Wireless Tokens)
  - Εικονικές συσκευές (Virtual Tokens)

Slide 9:

Συσκευές ασφαλείας

OTP , 2FA Tokens

One-time password Token

USB Token

Slide 10:

Συσκευές ασφαλείας

Βιομετρικοί σαρωτές

Οι Βιομετρικοί σαρωτές είναι συσκευές πιστοποίησης χρήστη και διαθέτουν έναν ή περισσότερους αισθητήρες κάποιου τύπου (οπτικό, υπέρυθρων, υπέρηχων) που λειτουργούν ως σαρωτές και μέσω των οποίων έχουν την δυνατότητα να αναλύουν διάφορα βιομετρικά χαρακτηριστικά του ανθρώπου. Η εξουσιοδότηση του χρήστη γίνεται βάση αποδεικτικών στοιχείων που δηλώνουν κάτι που ο χρήστης «είναι».

- **Βιομετρικός σαρωτής δακτυλικού αποτυπώματος**: χρησιμοποιεί έναν οπτικό σαρωτή ή σαρωτή υπέρηχων, για να διαβάζει και να αποθηκεύει δακτυλικά αποτυπώματα σε μια βάση δεδομένων. Εφαρμόζει αλγόριθμο αναγνώρισης προτύπων ή αλγόριθμο λεπτολογίας στα δακτυλικά αποτυπώματα, για να πιστοποιήσει την ταυτότητα του χρήστη

Slide 11:

Συσκευές ασφαλείας

Βιομετρικοί σαρωτές

- **Βιομετρικός σαρωτής παλάμης**: χρησιμοποιεί έναν οπτικό σαρωτή ή ένα σαρωτή υπέρυθρων μέσω του οποίου λαμβάνει διάφορες μετρήσεις όπως το μήκος, το πλάτος, το πάχος αλλά και την αναλογία της παλάμης για να πιστοποιήσει τον χρήστη. Συνοδεύονται με ένα μοναδικό κωδικό.
- **Βιομετρικός σαρωτής ίριδας**: χρησιμοποιεί μια κάμερα υψηλής ευκρίνειας με υπέρθυρο φωτισμό (μειώνει τις αντανακλάσεις) και αποτυπώνει με πολύ λεπτομερείς εικόνες τις σχηματικές δομές της ίριδας του ματιού.
- **Βιομετρικός σαρωτής προσώπου**: χρησιμοποιεί μια ή περισσότερες κάμερες υψηλής ευκρίνειας για να αποτυπώσει με λεπτομερείς εικόνες την σχετική θέση, μέγεθος και σχήμα που έχουν τα μάτια, η μύτη και το στόμα στο πρόσωπο.

Slide 12:

Συσκευές ασφαλείας

Βιομετρικοί σαρωτές

Slide 13:

Πλήρης κρυπτογράφηση δίσκου
με υλοποίηση λογισμικού

Η πλήρης κρυπτογράφηση δίσκου χρησιμοποιεί κατάλληλο λογισμικό ή υλικό για να κρυπτογραφήσει κάθε bit δεδομένων που βρίσκεται σε ένα δίσκο ή έναν τόμο του.

- **Πλήρης κρυπτογράφηση δίσκου με λογισμικό**:
  - Χρησιμοποιεί έναν αλγόριθμο κρυπτογράφησης ή ένα συνδυασμό αλγορίθμων που εφαρμόζονται σταδιακά, για να κρυπτογραφήσει όλα τα δεδομένα στον δίσκο, με το ίδιο κλειδί, σε επίπεδο λογισμικού.
  - Μειονέκτημα της, το γεγονός ότι αδυνατεί να κρυπτογραφήσει το πεδίο MBR των δίσκων. Το MBR περιέχει δεδομένα απαραίτητα για την εκκίνηση του λειτουργικού συστήματος, και πληροφορίες που περιγράφουν τις μονάδες στις οποίες ο δίσκος είναι χωρισμένος, αφήνοντας έτσι ένα μικρό αλλά σημαντικό κομμάτι του δίσκου ευάλωτο.

Slide 14:

Πλήρης κρυπτογράφηση δίσκου
με υλοποίηση υλικού

- **Πλήρης κρυπτογράφηση δίσκου με υλικό**:
  - Σκληροί δίσκοι FDE: είναι διαθέσιμοι σχεδόν από όλες τις εταιρίες κατασκευής σκληρών δίσκων. Η πιστοποίηση χρήστη γίνεται κατά την ενεργοποίηση του δίσκου σε περιβάλλον προ εκκίνησης. Η διαχείριση των κλειδιών γίνεται από τον ελεγκτή του δίσκου και χρησιμοποιεί κρυπτογραφικά κλειδιά αλγορίθμου AES.
  - Κρυπτο-επεξεργαστής TPM: ασφαλής κρυπτο-επεξεργαστής ενσωματωμένος στην μητρική πλακέτα του υπολογιστή, ο οποίος χρησιμοποιεί κρυπτογράφηση δημοσίου κλειδιού και έχει την δυνατότητα να δημιουργεί, να αποθηκεύει και να περιορίζει την χρήση κρυπτογραφικών κλειδιών.

Slide 15:

Πλήρης κρυπτογράφηση δίσκου

Σκληρός δίσκος FDE

TPM Chip

Slide 16:

Εφαρμογή πλήρους κρυπτογράφησης δίσκου με TrueCrypt

Τρόποι χρήσης:

- Δημιουργία κρυπτογραφημένης περιοχής
- Κρυπτογράφηση δίσκου/τόμου με ή χωρίς λειτουργικό σύστημα

Γενικές επιλογές:

- Κανονικός ή κρυφός τόμος.
- Κρυπτογράφηση ολόκληρου δίσκου ή ενός τόμου του.
- Υποστήριξη συστημάτων με ένα ή περισσότερα λειτουργικά συστήματα.

Slide 17:

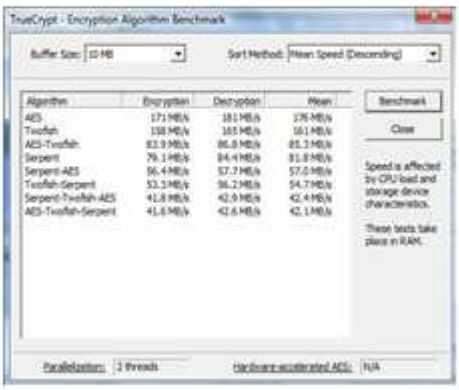
Εφαρμογή πλήρους κρυπτογράφησης δίσκου με TrueCrypt

Επιλογές κρυπτογράφησης:

- Αλγόριθμοι κρυπτογράφησης συμμετρικού κλειδιού: AES, Serpent, Twofish, και συνδυασμούς δύο ή τριών.
- Αλγόριθμοι κατακερματισμού: RIPEMD-160, SHA-512 και Whirlpool

Slide 18:

Εφαρμογή πλήρους κρυπτογράφησης δίσκου με TrueCrypt



Απόδοση συστήματος (Benchmark):

- Συσχετισμός επιθυμητού επιπέδου ασφάλειας, με απόδοση αλγορίθμων σε πραγματικό χρόνο.
- Ο συνδυασμός δύο ή περισσότερων αλγόριθμων προσφέρει υψηλότερα επίπεδα ασφάλειας, με κόστος όμως στις επιδόσεις του υπολογιστή και στον αρχικό χρόνο εφαρμογής.

Slide 19:

Εφαρμογή πλήρους κρυπτογράφησης δίσκου με TrueCrypt

Επιλογή κωδικού κρυπτογράφησης:

- Ο κωδικός πρέπει να αντιστέκεται σε εικασίες.
- Να μην αποτελείται από λέξεις ή συνδυασμό λέξεων που υπάρχουν σε γλωσσικά λεξικά.
- Να αποτελείται από ένα συνδυασμό τυχαίων χαρακτήρων, αριθμών και ειδικών συμβόλων.
- Όσο μεγαλύτερος τόσο ισχυρότερος.

Slide 20:

Εφαρμογή πλήρους κρυπτογράφησης δίσκου με TrueCrypt

Υποχρεωτική δημιουργία και εγγραφή δίσκου διάσωσης πριν την κρυπτογράφηση συστήματος.

Εμπεριέχει όλα τα κλειδιά κρυπτογράφησης.

Σε περίπτωση καταστροφής κρίσιμου λογισμικού της εφαρμογής, ή καταστροφικού προβλήματος στο λειτουργικό σύστημα, ο δίσκος διάσωσης μπορεί να επαναφέρει ή και να αποκρυπτογραφήσει πλήρως το σύστημα.

Slide 21:

Εφαρμογή πλήρους κρυπτογράφησης δίσκου με TrueCrypt

Προαιρετικές επιλογές:

- Σύνδεση κωδικού χρήστη με κρυπτογραφημένα αρχεία κλειδιά συσκευών ασφαλείας.
- Εφαρμογή αριθμού επαναλήψεων μεθόδου «κάθαρσης» στο δίσκο.

Η διαδικασία «κάθαρσης», εμποδίζει την ανάκτηση δεδομένων από μεθόδους μαγνητικής μικροσκοπίας.

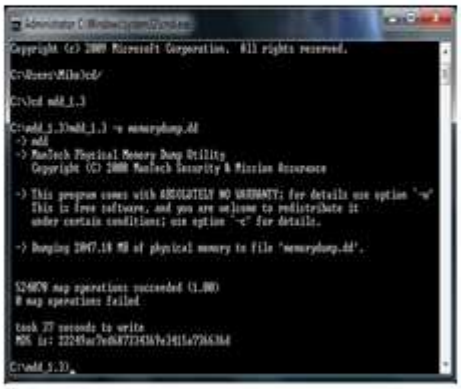
Slide 22:

Αδυναμίες ασφαλείας TrueCrypt

- Η ασφάλεια των δεδομένων βασίζεται στην μυστικότητα του κωδικού.
- Ευαισθησία σε μόλυνση συστήματος από κακόβουλο λογισμικό ή υλικό.
- Αδυναμία κρυπτογράφησης του πεδίου MBR του δίσκου. Πιθανή παράκαμψη κρυπτογραφίας με χρήση MBR rootkit.
- Πιθανή ανακάλυψη της ύπαρξης κρυπτογραφημένων τόμων με χρήση λογισμικού όπως το TCHunt.

Slide 23:

Αδυναμίες ασφαλείας TrueCrypt



- Το TrueCrypt εφαρμόζει την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων στην μνήμη του υπολογιστή.
- Με τη χρήση κατάλληλου λογισμικού, όπως το MDD, μπορεί ληφθεί ένα αντίγραφο μνήμης συστήματος και μέσω διαδικασιών ανάλυσης δεδομένων, είναι δυνατό να αποκαλυφθούν οι κωδικοί και τα κλειδιά κρυπτογράφησης.

Slide 24:

Συμπεράσματα και προτάσεις

- Όλες οι υλοποιήσεις ασφαλείας είναι πιθανό να είναι ευάλωτες.
- Για να επιτύχουμε υψηλά επίπεδα ασφάλειας σε ένα pc, είναι σημαντικό να συνδυάσουμε εφαρμογές και υλικό ασφαλείας, που δρα σε διαφορετικά επίπεδα.
- Ένας καλός συνδυασμός λογισμικού και υλικού ασφαλείας με χαμηλό κόστος επιτυγχάνεται με χρήση λογισμικού πλήρους κρυπτογράφησης δίσκου, αντιϊκού λογισμικού και μιας συσκευής ασφαλείας.
- Το TrueCrypt υποστηρίζει συνεργασία με συσκευές ασφαλείας που υλοποιούν το πρωτόκολλο PKCS#11 και νεότερες εκδόσεις του. Ενδεικτικά:
  - ASEKey Crypto USB Token, ePass1000 USB
  - IDProtect Smart Card και ASEDrive IIIe USB V2 Smart Card Reader
  - Eikon Digital Privacy Manager - USB fingerprint reader (*)

Slide 25:

Προστασία δεδομένων σε προσωπικούς υπολογιστές

Ευχαριστώ για τον χρόνο σας.

Ερωτήσεις;