Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων

Πτυχιακή εργασία

Τίτλος: *Μελέτη και δοκιμαστική λειτουργία των μηχανισμών ασφάλειας που παρέχει η πλατφόρμα Microsoft Windows Vista*

Όνομα Επίθετο: ΚΑΛΛΙΣΤΗ ΑΙΚΑΤΕΡΙΝΗ (ΑΜ: 674)

Ηράκλειο – Ημερομηνία
14/10/2008

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

Περιεχόμενα

1 ΠΡΟΛΟΓΟΣ 7

2 ΕΙΣΑΓΩΓΗ 8

3 ΟΙ ΕΚΔΟΣΕΙΣ ΤΩΝ WINDOWS VISTA 9

4 ΝΕΑ ΚΑΙ ΠΙΟ ΕΛΚΥΣΤΙΚΑ WINDOWS 11

4.1 Συνοπτικά οι νέοι μηχανισμοί ασφάλειας των Windows Vista. 12
4.1.1 User Account Control 12
4.1.2 Microsoft Internet Explorer (IE) 13
4.1.3 Windows Defender 14
4.1.4 Firewall filtering 14
4.1.5 Windows Service Hardening 15
4.1.6 Multi-Tiered Data Protection (Πολυστρωματική προστασία δεδομένων) 16
4.1.7 Network Access Protection (Προστασία πρόσβασης δικτύου) 16
4.1.8 Διαχειρισιμότητα 17
4.1.9 Αξιοπιστία και Απόδοση 20

5 ΚΕΝΤΡΟ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ WINDOWS VISTA 26

5.1 Περιγραφή του Κέντρου Ασφάλειας των Windows Vista 26
5.1.1 Αυτόματες Ενημερώσεις (Windows Update) 28
5.1.2 Τείχος προστασίας των Windows Vista - Firewall Windows. 33
5.1.3 Windows Defender 57

6 ΝΕΟΣ ΒΕΛΤΙΩΜΕΝΟΣ INTERNET EXPLORER 7 83

6.1 Εκδόσεις του Windows Internet Explorer 86

6.2 Χαρακτηριστικά ασφαλείας του Microsoft Internet Explorer 87
6.2.1 Phishing filter 87

7 ΕΠΙΠΛΕΟΝ ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΤΩΝ WINDOWS VISTA. 98

7.1 Γονικός Έλεγχος – User Account Control 98
7.1.1 Περιγραφή του UAC 98
7.1.2 Κατανόηση λογαριασμών χρήστη 101
7.1.3 Πως λειτουργεί ο γονικός έλεγχος. 107
7.1.4 Γονικός έλεγχος Βήμα-Βήμα 109
7.1.5 Πως ρυθμίζουμε τον Γονικό Έλεγχο 127

7.2 Κρυπτογράφηση συστήματος - BITLOCKER DRIVE ENCRYPTION 134
7.2.1 Τρόποι λειτουργιάς του Windows BitLocker. 135
7.2.2 Οδηγός Βήμα προς Βήμα του Windows BitLocker Drive Encryption 138

7.3 Windows service hardening 161
7.3.1 Ορισμοί συσχετιζόμενοι με την υπηρεσία Windows Hardening 162
7.3.2 Περιγραφή χαρακτηριστικών του Windows Service Hardening 175
7.3.3 Ο σκοπός της Υπηρεσίας Hardening. 175
7.3.4 Τι κάνει η Υπηρεσία Hardening. 176
7.3.5 Πως λειτουργεί το Windows Service Hardening. 177
7.3.6 Windows Service Hardening Στην πράξη. 183
7.3.7 Γιατί είναι σημαντική η υπηρεσία Windows Service Hardening 190

7.4 Επικύρωση - Authentication 191
7.4.1 Επικύρωση ενός αντικειμένου 192
7.4.2 Επικύρωση για την ασφάλεια του υπολογιστή 193

7.4.3 Επικύρωση ελέγχου πρόσβασης ... 193
7.4.4 Ορισμοί συσχετιζόμενοι με την Επικύρωση ... 194
7.4.5 Επικύρωση Διπλών παραγόντων (Two-factor authentication) ... 197
7.4.6 Επικύρωση της νέας γενιάς ... 206
7.4.7 Αναλυτική περιγραφή του μηχανισμού Επικύρωσης. ... 216
7.5 DRM Digital Rights Management. ... *251*
7.5.1 Τεχνολογίες όπου χρησιμοποιείται η DRM ... 252
7.5.2 Νόμοι σχετικοί με την DRM 254
7.5.3 Windows Media DRM 255
7.5.4 SKDs and Versions of Windows Media DRM. ... 259
7.5.5 Αρχιτεκτονική δομή του Windows Media Rights Manager. ... 264
7.5.6 Windows Media Rights Manager 10 SDK ... 267

8 Βιβλιογραφία ... 268

Πίνακας εικόνων

Εικόνα 1: Παρουσίαση συστατικών μιας πολιτικής περιορισμού λογισμικού 18
Εικόνα 2: Παράθυρο Κέντρου Ασφαλείας των Windows. 27
Εικόνα 3: Παράθυρο του Windows Update. 28
Εικόνα 4: Παράθυρο ελέγχου για ενημερώσεις των Windows 29
Εικόνα 5: Παράθυρο αλλαγή ρυθμίσεων του Windows Update. 30
Εικόνα 6 : Παράθυρο Επαναφορά κρυφών ενημερώσεων του Windows Update. 31
Εικόνα 7 : Παράθυρο προβολή ιστορικού ενημερώσεων τουWindows Update. 32
Εικόνα 8 : Τρόπος λειτουργίας του Windows Firewall 33
Εικόνα 9 : Κεντρικό παράθυρο του Windows Firewal 34
Εικόνα 10: Παράθυρο ρυθμίσεων του Windows Firewall. 35
Εικόνα 11:Πίνακας εξαιρέσεων του Windows Firewall 36
Εικόνα 12: Παράθυρο δημιουργίας εξαίρεσης από τον χρήστη. 37
Εικόνα 13: Παράθυρο προσθήκης θύρας TCP/UTP στις εξαιρέσεις του Windows Firewall. 38
Εικόνα 14: Καρτέλα για προχωρημένους χρήστες του Windows Firewall. 39
Εικόνα 15 : Παράθυρο ειδοποίησης του Windows Firewall. 41
Εικόνα 16 : Παράθυρο τείχος προστασίας των Windows με εξελιγμένη ασφάλεια 44
Εικόνα 17 : Παράθυρο τείχος προστασίας των Windows με εξελιγμένη ασφάλεια 46
Εικόνα 18 : Παράθυρο προειδοποίησης του τείχους προστασίας των Windows με εξελιγμένη ασφάλεια 46
Εικόνα 19 : Παράθυρο Άνοιγμα πολιτικής. 47
Εικόνα 20 : Παράθυρο τείχος προστασίας των Windows με εξελιγμένη ασφάλεια 48
Εικόνα 21: Παράθυρο Αποθήκευση πολιτικής 49
Εικόνα 22: Παράθυρο Οδηγού δημιουργίας κανόνα 50
Εικόνα 23: Παράθυρο Οδηγού δημιουργίας κανόνα 50
Εικόνα 24: Παράθυρο Οδηγού δημιουργίας κανόνα 51
Εικόνα 25: Παράθυρο Οδηγού δημιουργίας κανόνα 51
Εικόνα 26 : Παράθυρο Οδηγού δημιουργίας κανόνα 52
Εικόνα 27: Αρχικό παράθυρο του Windows Defender των Windows 59
Εικόνα 28 : Παράθυρο Εργαλεία του Windows Defender των Windows 60
Εικόνα 29: Παράθυρο Αρχική σελίδα του Windows Defender των Windows 62
Εικόνα 30 : Παράθυρο Σάρωσης του Windows Defender των Windows 63
Εικόνα 31 : Παράθυρο Ιστορικού του Windows Defender των Windows 66
Εικόνα 32: Παράθυρο Επιλογές του Windows Defender των Windows 75
Εικόνα 33 : Παράθυρο Αρχική σελίδα του Windows Defender των Windows 76
Εικόνα 34 : Παράθυρο Αρχική σελίδα του Windows Defender των Windows 78
Εικόνα 35: Παράθυρο εμφάνισης των Quick Tabs του Internet Explorer 7. 84
Εικόνα 36: Παράδειγμα 1ο Ιστοχώρος Phishing PayPal. 92
Εικόνα 37: Παράδειγμα 2ο Ιστοχώρος Phishing Barclays 93
Εικόνα 38 : Παράδειγμα 3ο Ιστοχώρος Phishing. 93
Εικόνα 39 : Παράδειγμα 4ο Υπόδειξη Ιστοχώρου Phishing 94
Εικόνα 40 : Παράδειγμα 5ο Υπόδειξη Ιστοχώρου Phishing 94
Εικόνα 41: Παράθυρο δημιουργίας νέου λογαριασμού χρήστη. 103
Εικόνα 42 : Παράθυρο τροποποίησης ονόματος χρήστη 104
Εικόνα 43 :Παράθυρο αλλαγής εικόνας του χρήστη. 104
Εικόνα 44 : Παράθυρο αλλαγής του τύπου του λογαριασμού χρήστη 105
Εικόνα 45 : Παράθυρο αλλαγής του κωδικού χρήστη. 106
Εικόνα 46 : Παράθυρο διαγραφής λογαριασμού χρήστη. 106
Εικόνα 47 : Παράθυρο πλαισίου μενού. 108
Εικόνα 48 : Κεντικό παράθυρο Γονικού Ελέγχου. 110
Εικόνα 49 : Παράθυρο ειδοποίησης. 111
Εικόνα 50 :Παράθυρο ειδοποίησης 112
Εικόνα 51 : Παράθυρα ειδοποιήσεων 114
Εικόνα 52 : Παράθυρο ειδοποίησης 115
Εικόνα 53 : Παράθυρο ειδοποίησης 115
Εικόνα 54 : Παράθυρο ειδοποίησης 116
Εικόνα 55: Παράθυρο πίνακα ελέγχου Ημερομηνίας και Ώρας 117
Εικόνα 56 : Παράθυρο επικύρωση εγκατάστασης 118
Εικόνα 57: Παράθυρο Τοπικής πολιτικής ασφάλειας 119

Εικόνα 58 : Παράθυρο Τοπικής πολιτικής ασφάλειας 120
Εικόνα 59: Παράθυρο ασφαλής επιφάνειας εργασίας 123
Εικόνα 60 : Παράθυρο Μενού 124
Εικόνα 61 : Παράθυρο Διαλόγου UAC 125
Εικόνα 62 : Παράθυρο Μενού 126
Εικόνα 63 : Παράθυρο Ιδιότητες 127
Εικόνα 64 : Παράθυρο επεξήγησης ρύθμισης γονικού ελέγχου για παιδιά 130
Εικόνα 65 : Παράθυρο ρύθμισης περιορισμού χρόνου 131
Εικόνα 66 : Παρουσίαση των τριών τρόπων λειτουργίας του Windows BitLocker 135
Εικόνα 67 : Περιγραφή του Διαφανή τρόπου λειτουργίας του Bitlocker Drive Encryption 136
Εικόνα 68 : Περιγραφή του τρόπου λειτουργίας του Bitlocker Drive Encryption με επικύρωση των χρηστών 137
Εικόνα 69 : Περιγραφή του τρόπου λειτουργίας του Bitlocker Drive Encryption με USB key. 137
Εικόνα 70 : Παρουσίαση των απαιτήσεων του συστήματος προσδιορισμού 139
Εικόνα 71 : Παρουσίαση προτεινόμενης σειράς λειτουργιών του BitLocker 139
Εικόνα 72 :Παράθυρο προετοιμασιας δίσκου για τον BitLocker 141
Εικόνα 73: Περιγραφή της αρχιτεκτονικής του BitLocker. 143
Εικόνα 74 : Περιγραφή της full-volume encryption 144
Εικόνα 75: Περιγραφή του διαγράμματος αρχιτεκτονικής του BitLocker 146
Εικόνα 76 : Παρουσίαση σεναρίου με χρήση TPM μόνο 148
Εικόνα 77: Παρουσίαση σεναρίου με ενισχυμένη επικύρωση 149
Εικόνα 78 :Παρουσίαση των τρόπων επικύρωσης του BitLocker 150
Εικόνα 79 : Σχεδιάγραμμα κύκλου ζωής του BitLocker 150
Εικόνα 80: Παράθυρο Έναρξης του BitLocker Drive Encryption 152
Εικόνα 81 : Παράθυρο παρουσίασης των τόμων (volumes) του BitLocker 153
Εικόνα 82 : Παράθυρο του Group Policy Object Editor 155
Εικόνα 83 : Παράθυρο ενεργοποίησης των προχωρημένων ρυθμίσεων. 156
Εικόνα 84 : Περιγραφή της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης 159
Εικόνα 85 : Καρτέλα Πίνακα Ελέγχου 164
Εικόνα 86 : Καρτέλα Εργαλεία Διαχείρισης. 165
Εικόνα 87 : Καρτέλα Υπηρεσίες. 165
Εικόνα 88: Παραθυρο εντολής sc.exe 184
Εικόνα 89 : Παράθυρο 1ο εμφάνιση λεπτομερειών μην περιορισμένης υπηρεσίας. 185
Εικόνα 90: Παράθυρο 2ο εμφάνιση λεπτομερειών περιορισμένης υπηρεσίας. 185
Εικόνα 91 : Παράθυρο εμφάνισης προσωπικής SID μιας περιορισμένης υπηρεσίας. 186
Εικόνα 92: Παράθυρο εμφάνισης προσωπικής SID μιας περιορισμένης υπηρεσίας. 186
Εικόνα 93 : Παράθυρο τροποποίησης προνομίων μιας υπηρεσίας. 188
Εικόνα 94 : Παράθυρο εμφάνισης αδειών πρόσβασης για το Windows Firewall. 190
Εικόνα 95 : Ψηφιακή υπογραφή 195
Εικόνα 96 : Παράδειγμα μιας έξυπνης κάρτας. 200
Εικόνα 97 : Παράδειγμα USB. 200
Εικόνα 98 : Έμπιστα σημεία ασφάλειας Identity Guard OTP 205
Εικόνα 99: Περιγαφή βιομετρικών συστημάτων 214
Εικόνα 100 :Δομή ενός PAP πακέτου 225
Εικόνα 101: Παραδείγματα CAPTCHA 234
Εικόνα 102 : Επικοινωνία μέσω πιστοποιητικών δημόσιου κλειδιού 236
Εικόνα 103 : Μηχανισμός Genuine Microsoft software 238
Εικόνα 104 : Μήνυμα ειδοποίησης του μηχανισμού WGA 239
Εικόνα 105 : Παράθυρο διαχείρησης των Internet Information Services (IIS). 240
Εικόνα 106 :User Authentication Servers configuration. 242
Εικόνα 107 : Ρύθμιση του User Authentication Server. 243
Εικόνα 108 : Παράθυρο ρυθμίσεων Κανόνων Επικύρωσης Χρήστη 244
Εικόνα 109 : Παράθυρο RADIUS Options 245
Εικόνα 110 : Παράθυρο ρυθμίσεων Agent Options 247
Εικόνα 111 :Παράθυρο ρυθμίσεων Περιορισμών 248
Εικόνα 112 : Παράθυρο επιλογή ενεργοποίησης XAUTH , σε ένα VPN τούνελ 249
Εικόνα 113 : Παράθυρο ενεργοποίησης επικύρωσης χρηστών , στα αντικείμενα δικτύου 250
Εικόνα 114 : Σχ. Παράθυρο ενεργοποίησης κανόνων που απαιτούν την επικύρωση των χρηστών 250
Εικόνα 115 : Απεικόνιση της αρχιτεκτονικής του Windows Media Rights Manager. 264

Εικόνα 116 : Περιγραφή της λειτουργίας του κλειδιού της άδειας που χρησιμοποιείται από τον Windows Media Rights Manager. 266

Πίνακας 1: Κατανόηση παραγόντων προστασίας σε πραγματικό χρόνο 71
Πίνακας 2: Κατανόηση των επιπέδων προειδοποίησης του Windows Defender. 80
Πίνακας 3 : Περιγραφή της σημασίας των χρωμάτων της γραμμής κατάστασης ασφαλείας 97
Πίνακας 4: Πολιτική συμπεριφοράς της προτροπής προβιβασμού 121
Πίνακας 5: Σενάριο γονικού ελέγχου χρήστη 130
Πίνακας 6 : Windows Vista Γονικοί Έλεγχοι 132
Πίνακας 7 : Πειγραφή των SIDs 167
Πίνακας 8: Σύγκρισης των βιομετρικών τεχνικών 212
Πίνακας 9: Συνδυασμοί τύπων πιστοποιητικών 228
Πίνακας 10 : Περιγραφή λειτουργιών της πλατφόρμας Media DRM 10. 260
Πίνακας 11 Εκδόσεις του Media DRM 262

1 ΠΡΟΛΟΓΟΣ

Ένα από τα σημαντικότερα θέματα που μας απασχολεί καθώς επιλέγουμε το λειτουργικό μας σύστημα είναι η ασφάλεια που αυτό μας παρέχει .Η επιλογή του εκάστοτε λογισμικού είναι άμεσα συνδεδεμένη με το ποσοστό ασφαλείας του . Οποιαδήποτε είδους διαρροή των δεδομένων μας , είτε αυτά είναι προσωπικά είτε επαγγελματικά μπορεί να αποβεί μοιραία ,επιφέροντας μας πολλά οικονομικά ή κοινωνικά προβλήματα .

Στις μέρες μας οι κίνδυνοι που παραμονεύουν είναι πολλοί και αυξάνουν συνεχώς. Άμεσο λοιπόν μέλημα μας είναι να προστατευθούμε όσο το δυνατόν περισσότερο μπορούμε . Πράγμα που συνεπάγει ότι θα πρέπει να ενημερωνόμαστε συνεχώς και να εξελισσόμαστε όσον το δυνατόν γρηγορότερα πάνω στα θέματα ασφάλειας. Επειδή όμως μαζί με μας εξελίσσονται και οι απειλές , για να μείνει προστατευμένο από τις απειλές που συναντά είτε στο διαδίκτυο είτε στα ασύρματα δίκτυα είτε άλλου, το λειτουργικό μας σύστημα πρέπει να εξελίσσετε και αυτό επίσης .

Τα Windows Vista ¨θεωρητικά¨ σχεδιάστηκαν για να είναι το ασφαλέστερο μέχρι στιγμής λειτουργικό σύστημα εν κυκλοφορία . Οι δημιουργοί των Vista Windows έδωσαν πολλοί προσοχή στα λάθη του παρελθόντος και προσπάθησαν να νικήσουν κάθε είδους απειλή . Παρόλα αυτά μέχρι και σήμερα είναι χαρακτηριστική η φράση που έχει επικρατήσει ότι τα «Vista έφτασαν, η ασφάλεια τους ..ακολουθεί» . Από την μεριά μας και εμείς ως σκεπτόμενοι και ευσυνείδητοι χρήστες θα πρέπει να λάβουμε τα μέτρα μας και να εφοδιάσουμε κατάλληλα τα συστήματα μας προκειμένου να καλύψουμε κάθε πιθανή «τρύπα» στην ασφάλεια του υπολογιστή μας .

Το αντικείμενο μελέτης της συγκεκριμένης πτυχιακής εργασίας είναι η μελέτη και η δοκιμή των δυνατοτήτων που παρέχουν τα Windows Vista στους χρήστες τους , για την προστασία της ταυτότητας τους , των δεδομένων τους καθώς και των επικοινωνιών τους .

2 ΕΙΣΑΓΩΓΗ

Η Microsoft έχει κάνει μια αξιοσημείωτη προσπάθεια έτσι ώστε να καταστήσει όσον το δυνατόν καλύτερα τους πελάτες τις ασφαλέστερους . Τα Windows Vista αποτελούν την πιο πρόσφατη έκδοση του λειτουργικού συστήματος της Microsoft. Διαθέτουν ένα ολοκληρωμένο σύστημα προστασίας και ασφαλείας των δεδομένων μας . Παρόλα αυτά πάντα θα υπάρχουν οι λεγόμενοι «κακόβουλοι» χρήστες που αναζητούν την «αχίλλειον φτέρνα» του εκάστοτε συστήματος ασφαλείας .

Γι αυτό κάθε ευσυνείδητος χρήστης θα πρέπει να είναι πάντα σε ετοιμότητα και να φροντίζει για την καλή συντήρηση της ασφάλειας του συστήματος του .

Μια σειρά από προγράμματα που εμπεριέχονται στα Vista και αναλαμβάνουν την προστασία μας από κάθε επίθεση είναι τα ακόλουθα:

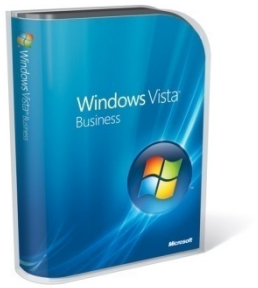
- **Δικτυακή προστασία (Windows Firewall).**
- **Έλεγχος και διαχείριση ενημερώσεων (Windows Update).**
- **Προστασία από επικίνδυνα προγράμματα (Windows Defender).**
- **Δικαιώματα πρόσβασης (User Account Control).**
- **Κέντρο ελέγχου για την ασφάλεια.**
- **Κρυπτογράφηση αρχείων και δίσκων (Bitlocker Drive Encryption).**
- **Σκλήρυνση υπηρεσιών Windows (Windows Service Hardening) .**
- **Μηχανισμός Επικύρωσης (Authentication).**

3 ΟΙ ΕΚΔΟΣΕΙΣ ΤΩΝ WINDOWS VISTA

Το νέο λειτουργικό της Microsoft είναι πλέον γεγονός. Στις 30 Ιανουαρίου 2007 κυκλοφόρησε η καινούργια έκδοση λειτουργικού συστήματος **Microsoft Windows** της Microsoft. Η νέα αυτή έκδοση φέρνει την ονομασία **Windows Vista** (ή αλλιώς με την κωδική ονομασία Longhorn) , κυκλοφόρησε σε πέντε διαφορετικές εκδόσεις ανάλογα με τις ανάγκες του εκάστοτε χρήστη.

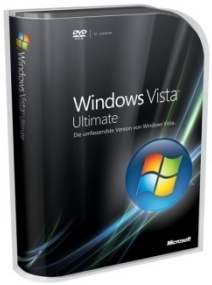
Τα **Windows Vista Home Basic**
Δεν έχουν καθοριστεί πηγές στο τρέχον έγγραφο. , απευθύνονται στους οικιακούς χρήστες διαθέτοντας το βασικό **User Interface** χωρίς να διαθέτουν το εντυπωσιακό **Aero Glass Interface ,** επιπλέον διαθέτουν τον **Windows Defender** το προηγμένο **Windows Firewall** και τον νέο και πιο ασφαλή **Internet Explorer 7** .

Η δεύτερη έκδοση είναι τα **Windows Vista Home Premium** και αυτή η έκδοση απευθύνεται σε τυπικούς χρήστες αλλά περιλαμβάνει τόσο το **Aero Glass Interface** , τον **Windows Defender**, το **Windows Firewall** ,τον **Internet Explorer 7** όσο και το **Media Center** αλλά και δυνατότητα υποστήριξη **Table Pc** και **HDTV**. Ένα νέο ακόμη χαρακτηριστικό είναι ο **Meeting Space** .



Τα **Windows Vista Business** είναι η τρίτη έκδοση των Windows Vista , απευθύνεται σε μικρές – μικρομεσαίες επιχείρησης και εκτός από τα προαναφερθέντα χαρακτηριστικά (Aero, Windows Defender ,Windows Firewall IE 7,Meeting Space, Table Pc και HDTV) είναι επιπλέον εξοπλισμένη με **εργαλεία λήψης αντιγράφων ασφαλείας** για επιχείρησης , σε περίπτωση κατάρρευσης του συστήματος μας με **Scheduled Backup** και το **Windows Complete Pc Backup and Restore**. Διαθέτει επίσης και τον **Internet Information Service Web (IIS 7.0)** και το **Windows Fax and Scan.** Τέλος αυτή η έκδοση διαθέτει κάποιες επιπλέον προηγμένες δυνατότητες δικτύωσης με το **Networking Center** και την δυνατότητα **Remote Desktop** .

Για τις εκδόσεις Home Basic και Business είναι διαθέσιμές και οι υποεκδόσεις N ,οι οποίες είναι οι ίδιες με τις κανονικές εκδόσεις με μόνη διαφορά ότι δεν διαθέτουν τον Windows Media Player.



Τελευταία θα αναφέρουμε την πιο πλήρη έκδοση των Windows Vista τα **Windows Vista Ultimate**, που απευθύνονται σε πιο έμπειρους χρήστες κυρίως σε επιχειρηματίες και σε φανατικούς χρήστες παιχνιδιών . Η έκδοση αυτή περιλαμβάνει τόσο τα χαρακτηριστικά των εκδόσεων Business και Home Premium και επιπλέον την δυνατότητα κρυπτογράφησης των δεδομένων μας για μεγαλύτερη ασφάλεια με το μηχανισμό **Windows BitLocker Drive Encryption** .

Τέλος στην τελευταία αυτή έκδοση συμπεριλαμβάνονται κάποιες επιπλέον δυνατότητες προηγμένης ψυχαγωγίας μετατρέποντας το συστημά μας σε κέντρο επεξεργασίας και αναπαραγωγής τόσο υψηλής ποιότητας ήχου όσο και εικόνας , με την βοήθεια των **Windows DVD Maker**, και **Windows Movie Maker in High Definition** .

Σε αυτό το σημείο θα πρέπει να αναφέρουμε ότι η πέμπτη έκδοση των Windows είναι διαθέσιμη μόνο εκτός Ελλάδας . Η έκδοση αυτή ονομάζεται **Starter**.

Στις 18 Μαρτίου 2008 η Microsoft κυκλοφόρησε και το **Service Pack 1** των Windows Vista , προκειμένου να καλύψει τα πρώτα κένα που διαπιστώθηκαν από τις μαρτυρίες των χρηστών . Περιλαμβάνει το Directx 10.1 που προσφέρει Mandatory 32-bit Floating point Filtering , Mandatory 4x , anti-aliasing και Shadel model 4.1.

Η Microsoft έχοντας επενδύσει πολλά σε αυτό το νέο λογισμικό , βρίσκεται σε συνεχή έρευνα ορθής λειτουργίας του, προκειμένου να βέλτιώσει, αν όχι να τελειοποιήσει , οποιοδήποτε ελλατωματικό σημείο των Windows Vista . Και υπόσχεται στους χρήστες τις την συνεχή βελτιστοποίηση τους .

4 ΝΕΑ ΚΑΙ ΠΙΟ ΕΛΚΥΣΤΙΚΑ WINDOWS

Οι απειλές της ασφάλειας του λειτουργικού μας συστήματος εξελίσσονται διαρκώς . Για να παραμείνουμε και εμείς ασφαλείς από τις απειλές που συναντάμε καθημερινά στο Ιντερνέτ καθώς και στα ασύρματα δίκτυα , το λειτουργικό μας σύστημα πρέπει και αυτό να εξελιχθεί . Η Microsoft αρχικά έκανε μια φιλότιμη προσπάθεια και αύξησε σημαντικά την ασφάλεια των Windows XP από την αρχική τους έκδοση , παρέχοντας ενημερώσεις όπως το Service Pack 2 . Όμως οι σημαντικές βελτιώσεις ασφαλείας απαιτούν σημαντικές αρχιτεκτονικές αλλαγές που μπορούν να πραγματοποιηθούν μόνο με μια νέα έκδοση λειτουργικού συστήματος .

Με τα νέα Windows Vista η Microsoft πραγματοποιεί θεμελιώδεις επενδύσεις στην τεχνολογία προκειμένου να ενισχύσει την ασφάλεια των πελατών της . Παρέχει την δυνατότητα στους μεγάλους οργανισμούς και στις επιχειρήσεις να επιτυγχάνουν τους υπολογιστικούς στόχους τους με αυτοπεποίθηση και με ένα ενισχυμένο αίσθημα ασφάλειας. Στις προσπάθειες περιλαμβάνονται η χρήση του **Security Development Lifecycle** για την ανάπτυξη ασφαλέστερου λογισμικού και η παροχή τεχνολογικής καινοτομίας στην πλατφόρμα για στρωματοποιημένη άμυνα ή άμυνα εις βάθος κατά των απειλών.

Τα Windows Vista περιλαμβάνουν πολλά χαρακτηριστικά και βελτιώσεις ασφαλείας για την προστασία των υπολογιστών από τις απειλές τελευταίας γενιάς, όπως τα spyware λογισμικά και γενικότερα άλλους τύπους κακόβουλου (malware) λογισμικού .

Τα Windows Vista προστατεύουν τις ιδιωτικές πληροφορίες , ενώ απομακρύνουν το λογισμικό υποκλοπής spyware με τον **Windows Defender** . Οι βελτιωμένες προσαρμοσμένες ρυθμίσεις **Γονικού Ελέγχου(User Account Control)** και ο νέος **Web Browser** της Microsoft , **Internet Explorer 7** με το ενσωματωμένο **Phishing Filter** ενισχύουν την ασφάλεια των χρηστών , καθώς εντοπίζουν και μπλοκάρουν τοποθεσίες με ακατάλληλο ή ύποπτο περιεχόμενο.

Ο **User Account Control** δίνει την δυνατότητα στους χρήστες να είναι περισσότερο παραγωγικοί , να μπορούν να προβούν άμεσα στις ρυθμίσεις κοινής χρήσης καθώς τρέχουν σε απλό λογαριασμό και χωρίς να απαιτούνται δικαιώματα διαχειριστή .
Αυτός ο μηχανισμός εμποδίζει τους χρήστες από το να κάνουν αλλαγές λόγο τις άγνοιας τους οι οποίες μπορούν να προβούν επικίνδυνες και επιβλαβής για τα συστήματα τους .

Ο **Windows Defender** εντοπίζει πολλών ειδών πιθανών ύποπτων λογισμικών , και αποτρέπει τους χρήστες για την χρήσης τους προτού αυτοί να επιτρέψουν στα λογισμικά αυτά να κάνουν οποιοδήποτε είδους κακόβουλες αλλαγές .

Ο νέος **Internet Explorer 7(IE)** περιλαμβάνει πολλές βελτιώσεις ασφαλείας οι οποίες προστατεύουν τους χρήστες από επιθέσεις ¨ψαρέματος¨ και πλαστογράφησης . Οι νέες αυτές βελτιώσεις περιλαμβάνουν ακόμη μια προστατευμένη λειτουργία του Internet Explorer , η οποία βοηθά στην προστασία τόσο των δεδομένων του χρήστη όσο και των ρυθμίσεων του από το να διαγραφούν ή να αλλαχθούν από κακόβουλα λογισμικά ή κακόβουλους δικτυακούς τόπους .

Το νέο **εξερχόμενο φιλτράρισμα** στο τείχος προστασίας είναι ένας ακόμη νέο και βελτιωτικός μηχανισμός ασφαλείας των Windows Vista . Ο μηχανισμός αυτός παρέχει διοικητικό έλεγχο πάνω από peer -to-peer εφαρμογές ανταλλαγής καθώς και άλλες παρόμοιες εφαρμογές που οι επιχειρήσεις θέλουν να περιορίσουν .

Ακολουθεί η υπηρεσία **Windows Service Hardening** , η οποία περιορίζει τις ζημιές που κακόβουλοι χρήστες προσπαθούν να δημιουργήσουν , μέσω της διαδικασίας ¨σκλήρυνσης των υπηρεσιών ¨. Θωρακίζοντας , λοιπόν τις υπηρεσίες με διάφορους κανόνες και προστατευτικούς μηχανισμούς τις κάνει λιγότερο ευπαθείς στις επιθέσεις .

Τα Windows Vista επέφεραν νέες ασφαλέστερες υπηρεσίες και στο κομμάτι της δικτύωσης μας . Οι διαχειριστές των μηχανημάτων μπορούν να χρησιμοποιήσουν την υπηρεσία με την ονομασία **Network Access Protection** . Η υπηρεσία αυτή αποτρέπει τους πελάτες των επιχειρήσεων, οι οποίοι δεν συμμορφώνονται με την επιτρεπτή εσωτερική πολιτική του συστήματος , να συνδεθούν με το εσωτερικό του δικτύου αποτρέποντας έτσι την εξάπλωση κακόβουλων λογισμικών και σε άλλους υπολογιστές .

Ο **BitLocker Drive Encryption** είναι ένας ακόμη νέο αξιοσημείωτος μηχανισμός ασφάλειας του νέου λειτουργικού . Ο μηχανισμός αυτός είναι ιδιαίτερα χρήσιμος στις επιχειρήσεις καθώς με την βοήθεια κατάλληλου υλικού γίνετε κρυπτογράφηση των προσωπικών δεδομένων των χρηστών με κυρίαρχο στόχο την προστασία τους . Η ενεργοποίηση του BitLocker Drive Encryption σε έναν υπολογιστή έχει σαν αποτέλεσμα την κωδικοποίηση όλου του όγκου δεδομένων που αυτό διαθέτει . Προστατεύοντας έτσι δεδομένα, αρχεία , e-mail καθώς και την πνευματική ιδιοκτησία από κακόβουλους χρήστες .

Τέλος για να εξασφαλιστεί ότι τα IT διαμερίσματα διαθέτουν ένα μεγάλο εύρος από μηχανισμούς επικύρωσης από τους οποίους μπορούν να επιλέξουν τον τρόπο με τον οποίον επιθυμούν να προστατευτούν, τα Windows Vista περιλαμβάνουν ακόμη την νέα **αρχιτεκτονική γνησιότητας** , η οποία είναι πολύ εύκολο να επεκταθεί ακόμη και από τρίτους προγραμματιστές .
Τέλος , έρχονται να προστεθούν στις ενέργειες αυτές και κάποιες ακόμη συσκευές ασφάλειας ή όπως αναφέρονται αλλιώς ισχυρές συσκευές ταυτοποίησης , όπως οι **έξυπνες κάρτες** ,τα αποτυπώματα scanners , και άλλες μορφές ισχυρής ταυτοποίησης .

Σαν αποτέλεσμα , με την ταυτόχρονη χρήση αυτών των συσκευών ασφάλειας οι χρήστες θα νιώσουν πιο ασφαλή , πιο ελεύθεροι και θα αποκτήσουν μεγαλύτερη αυτοπεποίθηση όσο αφορά την χρήση των υπολογιστών τους .

Παρακάτω θα ακολουθήσει λεπτομερή περιγραφή των πιο σημαντικών βελτιώσεων ασφαλείας των Windows Vista , τα πλεονεκτήματα που αυτά παρέχουν καθώς επίσης και τους λόγους που τα νέα αυτά χαρακτηριστικά είναι χρήσιμα τόσο για τους επαγγελματίες όσο και για τους απλούς χρήστες .

.

Τα νέα αυτά χαρακτηριστικά βελτιώσεων ασφάλειας περιγράφονται συνοπτικά παρακάτω στην συνέχεια της εργασίας θα ακολουθήσει λεπτομερής περιγραφή τους :

4.1 Συνοπτικά οι νέοι μηχανισμοί ασφάλειας των Windows Vista.

4.1.1 User Account Control

Με τα Windows XP και τα παλαιότερα λειτουργικά συστήματα , τα τμήματα IT έπρεπε να διαλέξουν μεταξύ της συμβατότητας και ευχρηστίας των εφαρμογών (τα οποία επιτυχαίνονταν με σύνδεση του χρήστη με δικαιώματα διαχειριστή) και τις παρεχόμενης ασφάλειας και

σταθερότητας των συστημάτων (τα οποία ήταν αποτέλεσμα της σύνδεσης του χρήστη με δικαιώματα τυπικού χρήστη) . Το νέο χαρακτηριστικό User Account Control στα Windows Vista παρέχει στους διαχειριστές την δυνατότητα επιλογής δικαιωμάτων περιορισμού ενώ εξακολουθεί να επιτρέπει την λειτουργία των περισσότερων εφαρμογών.

Για να συμβάλουν στην παροχή αυτού του συνδυασμού ασφάλειας και συμβατότητας , τα Windows Vista χρησιμοποιούν το χαρακτηριστικό **File & Registry Virtualization** το οποίο αναλαμβάνει να ανακατευθύνει αυτόματα , να γράφει και κατόπιν να προσπελαύνει περιοχές που ο τυπικός χρήστης δεν έχει άδεια πρόσβασης . Οι αλλαγές που γίνονται στις ρυθμίσεις και τους φακέλους του ιδεατού μητρώου (virtualized registry) είναι ορατές μόνο στο συγκεκριμένο λογαριασμό χρήστη και στις εφαρμογές που χρησιμοποιεί ο χρήστης , επομένως η ακεραιότητα του υπολογιστή προστατεύεται .

Εάν μια εφαρμογή απαιτεί δικαιώματα διαχειριστή , τα Windows Vista θα ζητήσουν από το χρήστη την απαραίτητη πιστοποίηση πριν επιτρέψουν την λειτουργία της εφαρμογής . Αυτός ο τρόπος λειτουργίας , μέσω αυτού του νέου μηχανισμού αποτρέπει τους χρήστες να κάνουν ενδεχομένως επικίνδυνες για το σύστημά τους αλλαγές , με σημαντικότερο το γεγονός ότι δεν περιορίζεται η ικανότητα του χρήστη να τρέχει όποια εφαρμογή και αν αυτός επιθυμεί .

4.1.2 Microsoft Internet Explorer (IE)

Ο Internet Explorer που είναι ενσωματωμένος στα Windows Vista περιλαμβάνει πολλά ακόμη νέα χαρακτηριστικά ασφάλειας και πολλές έξτρα λειτουργίες οι οποίες προστατεύουν τους χρήστες και τα δεδομένα τους από πλήθος επιθέσεων όπως για παράδειγμα η αποτροπή επίσκεψης των χρηστών σε κακόβουλα sites καθώς προστατεύεται επίσης από επιθέσεις της μορφής malware , spoofing ή phishing . Τα νέα αυτά χαρακτηριστικά συμπεριλαμβάνονται στην νέα προστατευμένη μορφή του Internet Explorer , η οποία βοηθάει να προστατευτούν τόσο τα δεδομένα των χρηστών καθώς επίσης αποτρέπει να αλλαχθούν ή να διαγραφούν οι ρυθμίσεις διαμόρφωσης τις οποίες έχουν ρυθμίσει οι χρήστες , από κακόβουλα web site ή malware .

Τα Windows Vista όπως προαναφέραμε στηρίζονται στο χαρακτηριστικό Ελέγχου Λογαριασμού Χρήστη (User Account Control) προκειμένου να ορίσουν την λειτουργία του Internet Explorer με τα απολύτως απαραίτητα δικαιώματα που απαιτούνται για την περιήγηση στο Web, χωρίς όμως να επιτρέπεται τροποποίηση των αρχείων ή των ρυθμίσεων του χρήστη . Αυτό το χαρακτηριστικό το διαθέτουν μόνο τα Windows Vista , και είναι γνωστό και ως **Κατάσταση Προστατευμένης Λειτουργίας (Protected Mode)**. Επομένως , ακόμη κι αν μια τοποθεσία με κακόβουλο λογισμικό επιτεθεί σε μια πιθανή αδυναμία του Internet Explorer , ο κώδικας της τοποθεσίας δεν θα έχει αρκετά δικαιώματα πρόσβασης ώστε να εγκαταστήσει λογισμικό , να αντιγράψει αρχεία στον φάκελο εκκίνησης (Startup Folder) του χρήστη ή να αλλοιώσει τις ρυθμίσεις για την αρχική σελίδα του προγράμματος περιήγησης ή τον πάροχο αναζητήσεων (Search provider) .

Για να συμβάλει στην προστασία των ατομικών πληροφοριών ενός χρήστη , ο Internet Explorer :

- Επισημαίνει τη νέα γραμμή κατάστασης ασφάλειας (security status bar) όταν ο χρήστης επισκέπτεται μια τοποθεσία στο διαδίκτυο η οποία προστατεύεται με χρήση **Secure Sockets Layer – SSL** και επιτρέπει στο χρήστη να ελέγχει την εγκυρότητα του πιστοποιητικού ασφάλειας μιας τοποθεσίας.

- Διαθέτει φίλτρο κατά του **phishing** , που βοηθά τους χρήστες να πραγματοποιούν πιο ασφαλείς περιηγήσεις ενημερώνοντας τους πότε τοποθεσίες Web επιχειρούν να κλέψουν τις εμπιστευτικές πληροφορίες τους .Το φίλτρο λειτουργεί αναλύοντας το περιεχόμενο της τοποθεσίας , αναζητώντας γνωστά χαρακτηριστικά τεχνικών phishing και χρησιμοποιώντας ένα διεθνές δίκτυο πηγών δεδομένων για να αποφασίσει εάν ο χρήστης πρέπει να εμπιστευτεί την τοποθεσία Web . Τα φίλτρα ενημερώνονται αρκετές φορές κάθε ώρα , γεγονός σημαντικό με δεδομένη την ταχύτητα εμφάνισης των τοποθεσιών phishing και της ενδεχόμενης συλλογής των δεδομένων του χρήστη .
- Εκκαθαρίζει όλα τα δεδομένα που έχουν αποθηκευτεί στην μνήμη cache με ένα απλό κλικ.

4.1.3 Windows Defender

Το τρίτο νέο χαρακτηριστικό ασφάλειας των Windows Vista είναι ο **Windows Defender**. Το χαρακτηριστικό User Account Control , το οποίο περιγράφεται παραπάνω , καθώς και οι βελτιώσεις ασφάλειας στον Internet Explorer (συμπεριλαμβανομένου και του νέου Protected Mode) μπορούν να περιορίσουν το κακόβουλο και μη ανεπιθύμητο λογισμικό στα Windows Vista .

Εκτός από αυτά τα χαρακτηριστικά, τα Windows Vista μπορούν να ανιχνεύσουν και να εκκαθαρίσουν πολλές εφαρμογές κακόβουλου λογισμικού , όπως λογισμικό υποκλοπής (spyware) και άλλο ενδεχομένως ανεπιθύμητο λογισμικό με το Windows Defender , αλλά και το **Εργαλείο Κατάργησης Κακόβουλου Λογισμικού (Malicious Software Removal Tool - MSRT)** το οποίο ανανεώνεται σε μηνιαία βάση μέσω των Αυτόματων Ενημερώσεων (Automatic Updates - AU) . Αυτές οι τεχνολογίες συμβάλουν στην προστασία της ακεραιότητας του λειτουργικού συστήματος και στην εμπιστευτικότητα των δεδομένων των χρηστών.

Παρόλο που τα Windows Vista περιλαμβάνουν πολλές τεχνολογίες προστασίας από κακόβουλα λογισμικά, για βέλτιστη προστασία συνιστάται μια πλήρης λύση προστασίας από ιούς . Σημειώνεται εδώ πως το ενσωματωμένο σύστημα ανίχνευσης , εκκαθάρισης και αποκλεισμού , σε πραγματικό χρόνο , του κακόβουλου λογισμικού , στοχεύει κυρίως σε χρήστες που δεν διαθέτουν διαχείριση ασφάλειας (unmanaged users). Τα Windows Vista περιλαμβάνουν ακόμη κάποια άλλη υποστήριξη , σε εταιρικό επίπεδο, για τη διαχείριση των μέσων προστασίας από κακόβουλο λογισμικό μέσω **ομαδικών πολιτικών (group policies)**, πέρα από την αντιμετώπιση προβλημάτων (troubleshooting) και την ενεργοποίηση/απενεργοποίηση του Windows Defender.

4.1.4 Firewall filtering

Το νέο **¨αμφίδρομο¨ φιλτράρισμα** (εισερχόμενο - εξερχόμενο) που έχει προστεθεί στο τείχος προστασίας (firewall) του λογισμικού μας είναι ένα ακόμη επιπρόσθετο χαρακτηριστικό ασφάλειας το οποίο είναι ιδιαίτερα χρήσιμο στις μεγάλες επιχειρήσεις γιατί παρέχει διοικητικό έλεγχο ιδιαίτερα πάνω στις peer-to-peer sharing εφαρμογές αλλά και σε άλλες παρόμοιες εφαρμογές τις οποίες οι επιχειρήσεις θέλουν να περιορίσουν .

Το firewall που είναι ενσωματωμένο στα Windows Vista βασίζεται και επεκτείνει τη λειτουργικότητα που αρχικά προσφέρθηκε με το Microsoft Windows XP Service Pack 2. Για

παράδειγμα , το firewall των Windows Vista μπλοκάρει όλα τα εισερχόμενα μηνύματα έως ότου εγκατασταθούν στον υπολογιστή οι τελευταίες ενημερώσεις ασφαλείας. Το αμφίδρομο όπως προαναφέραμε firewall περιλαμβάνει , επίσης , φιλτράρισμα και της εξερχόμενης κίνησης, επιτρέποντας έτσι στους χρήστες να το διαμορφώνουν ώστε να μπλοκάρουν επιλεκτικά τόσο την εισερχόμενη όσο και την εξερχόμενη κίνηση .
Κάθε χαρακτηριστικό του firewall των Windows Vista μπορεί να διαμορφωθεί μέσα από τις ρυθμίσεις του Group Policy, επομένως οι ρυθμίσεις ασφαλείας του υπολογιστή παραμένουν σταθερές . Για πρώτη φορά σε ένα λειτουργικό σύστημα των Windows , η διαχείριση του firewall των Windows Vista ενσωματώνεται με το IPSec. Στα Windows Vista , το Internet Protocol security(IPSec) και η διαχείριση του firewall ενσωματώνονται σε μια κονσόλα , που είναι γνωστή ως Windows Firewall with Advanced Security (Windows Firewall με προηγμένη ασφάλεια). Αυτή η κονσόλα αποτελεί μια κεντρική θέση στο περιβάλλον εργασίας για το φιλτράρισμα εισερχόμενων και εξερχόμενων μηνυμάτων μαζί με τις ρυθμίσεις απομόνωσης του IPSec σε επίπεδο τομέα (IPSec domain isolation settings), επιτρέποντας αυξημένη και πιο εύκολη επίβλεψη των ρυθμίσεων ασφάλειας
Το firewall συνεργάζεται ακόμη με την λειτουργία Windows Service Hardening , αναλυτικά για αυτήν την λειτουργία θα αναφερθούμε παρακάτω.

4.1.5 Windows Service Hardening

Το νέο αυτό χαρακτηριστικό έχει την δυνατότητα να περιορίσει τις ζημιές που μπορούν να προκαλέσουν μιας ειδικής κατηγορίας επιτιθέμενοι , οι οποίοι είναι σε θέση να ¨συμβιβάσουν¨ επιτυχώς μια υπηρεσία . Κατά συνέπεια , ο κίνδυνος από αυτού του είδους επιτιθέμενους οι οποίοι προκαλούν μόνιμες αλλαγές στα Windows Vista client ή οι επιθέσεις που επιχειρούνται σε άλλους υπολογιστές των δικτύων αυτών , μειώνονται αισθητά .
Ακόμη όπως προαναφέραμε το firewall συνεργάζεται με την λειτουργία Windows Service Hardening ώστε να περιορίζει τις αλλαγές που μπορούν να γίνουν στο σύστημα από τις διάφορες υπηρεσίες (Computer Services) , παρέχοντας άμυνα εις βάθος και μειώνοντας τις ευκαιρίες που έχουν οι εισβολείς να επιτεθούν σε ευάλωτα σημεία των συστημάτων μας .

Το Windows Service Hardening δεν επιτρέπει σε κρίσιμες υπηρεσίες των Windows να πραγματοποιούν ασυνήθιστες δραστηριότητες στο σύστημα αρχείων , το μητρώο (registry), το δίκτυο ή σε άλλους πόρους που θα μπορούσαν να χρησιμοποιηθούν για να επιτρέψουν την εγκατάσταση κακόβουλου λογισμικού ή την επίθεση σε άλλους υπολογιστές . Για παράδειγμα ,η υπηρεσία Remote Procedure Call (RPC) μπορεί να μπλοκαριστεί ώστε να μπορεί να αντικαταστήσει αρχεία συστημάτων ή να τροποποιήσει το μητρώο.

Τέλος με την χρήση διαφόρων τεχνικών ο μηχανισμός αυτός ¨σκληραίνει¨ και θωρακίζει τις υπηρεσίες τόσο των χρηστών αλλά κυρίως του συστήματος , αποτρέποντας έτσι την ασυνείδητη εκμετάλλευση τους .

4.1.6 Multi-Tiered Data Protection (Πολυστρωματική προστασία δεδομένων)

Η κλοπή ή η απώλεια εταιρικής πνευματικής ιδιοκτησίας είναι ένα πρόβλημα που απασχολεί όλο και περισσότερο τους οργανισμούς . Τα Windows Vista διαθέτουν βελτιωμένη υποστήριξη για προστασία δεδομένων σε επίπεδα εγγράφων, αρχείων, καταλόγου και υπολογιστή . Το ενσωματωμένο πρόγραμμα Διαχείρισης Δικαιωμάτων (Rights Management Client) επιτρέπει στους οργανισμούς να επιβάλλουν πολιτικές σχετικά με την χρήση των εγγράφων . Το Κρυπτογραφημένο File System (Encrypted File System - EFS) , το οποίο παρέχει κρυπτογράφηση αρχείων και καταλόγου βάσει χρήστη , έχει βελτιωθεί ώστε να επιτρέπει την αποθήκευση κλειδιών σε smart cards , παρέχοντας καλύτερη προστασία των κλειδιών κρυπτογράφησης . Επιπλέον, το νέο εταιρικό χαρακτηριστικό Bit Locker Drive Encryption προσθέτει προστασία δεδομένων σε επίπεδο υπολογιστή . Παρέχει πλήρη κωδικοποίηση του δίσκου στον οποίο είναι εγκατεστημένο το σύστημα, συμπεριλαμβανομένων των αρχείων του συστήματος Windows και αρχείου αδρανοποίησης (hibernation), συμβάλλοντας έτσι στην προστασία δεδομένων σε περίπτωση απώλειας , κλοπής ή βλάβης του υπολογιστή.

Μια λύση με δυνατότητες εύκολης ανάπτυξης και διαχείρισης , είναι αυτή στην οποία χρησιμοποιείται ένα τσιπ Trusted Platform Module (TPM) 1.2 για την αποθήκευση κλειδιών που κρυπτογραφούν και αποκρυπτογραφούν τομείς στον σκληρό δίσκο των Windows . Για να διασφαλιστεί ότι το χαρακτηριστικό μπορεί να χρησιμοποιηθεί εύκολα από τους τελικούς χρήστες , απαιτείται εκτός από το TPM και μια υποδομή διαχείρισης του σε εταιρικό επίπεδο .

4.1.7 Network Access Protection (Προστασία πρόσβασης δικτύου)

Τα Windows Vista περιλαμβάνουν έναν πράκτορα (agent) που μπορεί να δίνει πληροφορίες σχετικά με την κατάσταση λειτουργίας και την διαμόρφωση του υπολογιστή σε εξυπηρετητές (servers) ή άλλους πελάτες- clients (peers) που έχουν πρόσβαση στο δίκτυο. Με το χαρακτηριστικό **Network Access Protection** οι υπολογιστές που δεν διαθέτουν τις τρέχουσες ενημερώσεις ασφάλειας , τις υπογραφές ιών ή με άλλα λόγια δεν πληρούν τις απαιτήσεις για την καλή λειτουργία του υπολογιστή δεν μπορούν να επικοινωνήσουν με το ιδιωτικό δίκτυο.
Το Network Access Protection μπορεί να χρησιμοποιηθεί για την προστασία του ιδιωτικού δικτύου ενός οργανισμού από την απομακρυσμένη πρόσβαση υπολογιστών καθώς και υπολογιστές του τοπικού δικτύου (LAN) μέσω ενσύρματων ή ασύρματων συνδέσεων . Ο agent αναφέρει σε ένα Service του Server που απασχολείται με την επιβολή του Network Access Protection, την κατάσταση λειτουργίας του υπολογιστή με Windows Vista, δηλαδή αναφέρει αν υπάρχουν εγκατεστημένες οι τρέχουσες ενημερώσεις και οι ενημερωμένες υπογραφές ιών. Μια υποδομή με Network Access Protection, που περιλαμβάνεται στον Windows Server με κωδικό όνομα ¨ Longhorn¨, προσδιορίζει εάν θα χορηγηθεί ή πρόσβαση client στο ιδιωτικό σας δίκτυο ή σε περιορισμένο δίκτυο.

Τέλος ένα επιπλέον χαρακτηριστικό ασφαλείας είναι οι νέες δυναμικές δυνατότητες και δικαιώματα που έχουν οι διαχειριστές του συστήματος. Για παράδειγμα οι διαχειριστές μπορούν να χρησιμοποιήσουν την προστασία πρόσβασης στο δίκτυο (Network Access Protection) για να απαγορέψουν τους απλούς χρήστες , οι οποίοι δεν υπακούον στην πολιτική ασφαλείας του συστήματος , από το να συνδεθούν στο εσωτερικό του δικτύου και ενδεχομένως έτσι να συντελέσουν στην εξάπλωση malware και σε άλλους υπολογιστές .

4.1.8 Διαχειρισιμότητα

Τα Windows Vista εκφράζουν ένα σημαντικό βήμα προόδου και σε άλλους τομείς εκτός από την ασφάλεια όπως πχ στην αξιοπιστία , απόδοση και διαχειρισιμότητα. Τομείς που είναι άμεσα συνδεδεμένοι με ην ασφάλεια του συστήματος και σε συνδυασμό με αυτής θωρακίζουν την άμυνα του υπολογιστή.
Παρακάτω θα αναφερθούν περιληπτικά ορισμένες από τις νέες βελτιωμένες ρυθμίσεις των Windows Vista .

Η παρακολούθηση, η διατήρηση και η αντιμετώπιση προβλημάτων σε εκατοντάδες ή χιλιάδες υπολογιστές μπορεί να αποβεί χρονοβόρα και δαπανηρή. Τα Windows Vista σημείωσαν ένα σημαντικό βήμα προόδου στο πλαίσιο της δέσμευσης της Microsoft για την μείωση του συνολικού κόστους ιδιοκτησίας (Total Cost of Ownership - TCO) των Windows . Τα Windows Vista έχουν σχεδιαστεί ώστε να μειώνουν το κόστος υποστήριξης του επιτραπέζιου υπολογιστή (desktop) , να απλοποιούν τη διαχείριση διαμόρφωσης του επιτραπέζιου υπολογιστή , να επιτρέπουν την κεντρικότερη διαχείριση διαμόρφωσης της επιφάνειας εργασίας και να μειώνουν το κόστος διαρκούς ενημέρωσης των συστημάτων .
Χάρη στις επεκτεινόμενες ρυθμίσεις των Group Policies, σχεδόν κάθε πλευρά των Windows Vista μπορεί να διαμορφωθεί από ένα κεντρικό σημείο , ενώ τα ισχυρά εργαλεία γραμμής εντολών και χρήσης script επιτρέπουν στους IT επαγγελματίες να αυτοματοποιούν μονότονες εργασίες. Η παρακολούθηση και η δημιουργία αναφορών είναι, επίσης , δυνατό να πραγματοποιηθεί από ένα κεντρικό σημείο.

4.1.8.1 Configuration Management (Διαχείριση Διαμόρφωσης)

Η τεχνολογία των Windows Vista διασφαλίζει ότι οι αλλαγές στα αρχεία και τις ρυθμίσεις των Windows πραγματοποιούνται με προβλέψιμο και αξιόπιστο τρόπο . Η τεχνολογία **Windows Resource Protection** (WRP) επιτρέπει στο σύστημα να προστατεύεται από ανεπιθύμητες αλλαγές σε αρχεία συστήματος , φακέλους ή κλειδιά μητρώου (registry keys) αλλαγές που μπορούν να θέσουν έναν υπολογιστή ή μια εφαρμογή εκτός λειτουργίας . Οι ρυθμίσεις συστήματος στο μητρώο προστατεύονται από ακούσιες αλλαγές που μπορούν να γίνουν από χρήστες ή μη εξουσιοδοτημένο λογισμικό. Μόνο ένας ¨έμπιστος ¨ (trusted) Windows Installer μπορεί να κάνει αλλαγές σε προστατευμένα αρχεία και ρυθμίσεις συστήματος.

4.1.8.2 Group Policies (Πολιτικές Ομάδων)

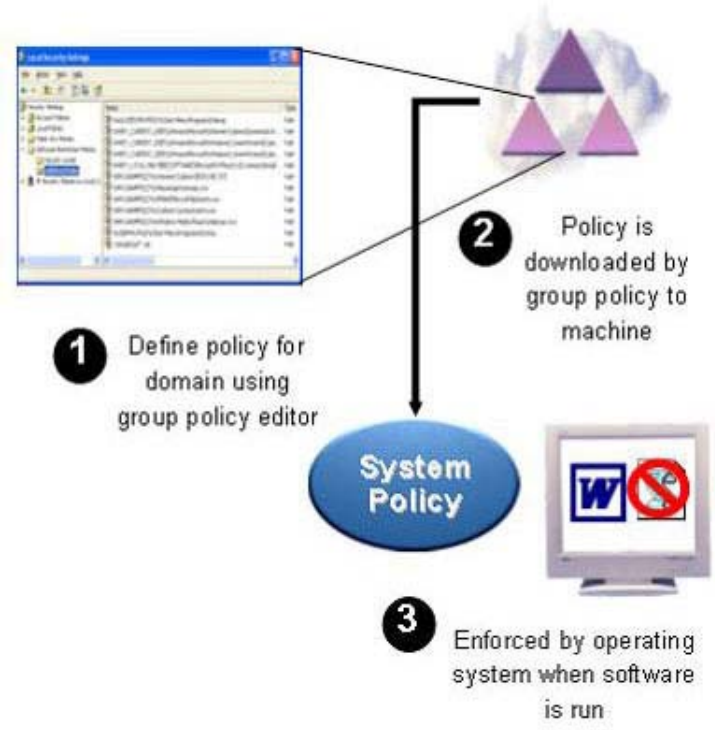
Σχεδόν κάθε νέα ρύθμιση διαμόρφωσης στα Windows Vista μπορεί να ελεγχθεί μέσω Group Policies . Επίσης , η **Κονσόλα Διαχείρισης Πολιτικής Ομάδας (Group Policy Management Console - GPMC)** περιλαμβάνεται τώρα στα Windows Vista. Για να γίνουν πιο ευέλικτα τα Windows Vista σε περιβάλλοντα όπου πολλαπλοί χρήστες χρησιμοποιούν έναν υπολογιστή , όπως σε σχολεία και βιβλιοθήκες , τα Windows Vista μπορούν να εφαρμόσουν πολλαπλά αντικείμενα Τοπικών (local) Group Policies . Αυτό το χαρακτηριστικό βελτιώνει την ασφάλεια και την διαχειρισιμότητα σε περιβάλλοντα κοινής χρήσης.

4.1.8.3 Policy – based Quality of Service (Ποιότητα Υπηρεσιών βάση πολιτικών)

Με την ποιότητα υπηρεσιών (QoS) βάσει πολιτικών , ένα εταιρικό τμήμα IT είναι σε θέση να ορίζει ευέλικτες πολιτικές ποιότητας υπηρεσιών ώστε να θέτει προτεραιότητες ή / και να επιταχύνει εξερχόμενα μηνύματα δικτύου χωρίς να απαιτούνται τροποποιήσεις σε εφαρμογές. Αυτές οι πολιτικές QoS θα εφαρμόζονται σε εξερχόμενα μηνύματα βάσει κάποιας από τις παρακάτω συνθήκες ή και όλων των συνθηκών : εφαρμογή αποστολής, εγκατάσταση λογισμικού μέσω Group Policies (σε ομάδες χρηστών ή υπολογιστών), διεύθυνση IP προέλευσης / προορισμού, θύρα προέλευσης/ προορισμού και πρωτόκολλα.

4.1.8.3.1 Αρχιτεκτονική πολιτικής περιορισμού λογισμικού .

Στο σχήμα που ακολουθεί παρουσιάζονται τα τρία συστατικά μιας πολιτικής περιορισμού λογισμικού .



Εικόνα 1: Παρουσίαση συστατικών μιας πολιτικής περιορισμού λογισμικού .

1. Ένας διαχειριστής δημιουργεί μια πολιτική , χρησιμοποιώντας την Group Policy Microsoft Console(MMC) , για ένα ιδιαίτερο Active Directory site ,ένα domain , ή μια οργανωτική μονάδα (OU).
2. Η πολιτική κατεβάζεται και εφαρμόζεται σε μια μηχανή . Οι πολιτικές χρηστών εφαρμόζονται την επόμενη φορά που ένας νέος χρήστης συνδέεται. Οι πολιτικές μηχανών ισχύουν όταν αρχίζει μια συσκευή .
3. Όταν ένας χρήστης αρχίζει ένα πρόγραμμα ή ένα χειρόγραφο , το λειτουργικό σύστημα ή ο scripting host ελέγχει την πολιτική και την επιβάλλει .

4.1.8.4 Αναφορά συμβάντων και αναφορά σφαλμάτων

Η διαχείριση των Windows Vista είναι ευκολότερη , εξοικονομώντας χρόνο και κόπο για τους IT επαγγελματίες . Οι περιγραφές συμβάντων (events) περιέχουν περισσότερα δεδομένα που βοηθούν στον εντοπισμό της βασικής αιτίας ενός προβλήματος και περιέχουν πληροφορίες για το συμβάν σε μορφή XML , διευκολύνοντας την προβολή των δεδομένων των συμβάντων τα οποία αξιοποιούνται από τα εργαλεία διαχείρισης . Για συνήθη προβλήματα , η διαδικασία μπορεί να αυτοματοποιηθεί ώστε να γίνεται εκκίνηση ενεργειών όταν εμφανίζεται ένα συγκεκριμένο συμβάν . Τα Windows Vista καθιστούν ευκολότερη την χειροκίνητη ανάλυση συμβάντων , επιτρέποντας στον χρήστη να προσαρμόζει τον τρόπο εμφάνισης των συμβάντων από το Event Viewer (Πρόγραμμα Προβολής Συμβάντων). Επίσης , τα Windows Vista μπορούν να προωθήσουν συμβάντα σε μια κεντρική τοποθεσία ώστε να διευκολύνεται ο προσδιορισμός , η παρακολούθηση και η αντιμετώπιση προβλημάτων.

4.1.8.5 Αυτοματοποίηση

Οι δυνατότητες αυτοματοποίησης των Windows Vista επιτρέπουν την πραγματοποίηση επαναλαμβανόμενων διαχειριστικών εργασιών χωρίς παρέμβαση του χρήστη, περιορίζοντας την πιθανότητα μη αυτόματων σφαλμάτων. Τα Windows Vista προσθέτουν αρκετές, σημαντικές δυνατότητες αυτοματοποίησης:

- Το πρωτόκολλο Web Services for Management (WS-Management), ένα industry-standard Web Services πρωτόκολλο για προστατευμένη απομακρυσμένη διαχείριση υλικού και λογισμικού, καθιστά τη διαχείριση των Windows Vista ευκολότερη σε ένα δίκτυο επιτρέποντας στους διαχειριστές να χρησιμοποιούν scripts και να εκτελούν άλλες ενέργειες διαχείρισης εξ αποστάσεως.

- Βασικές διαχειριστικές εργασίες, που είναι δυνατό να εκτελεστούν από ένα περιβάλλον εργασίας (User Interface - UI), μπορούν επίσης να ολοκληρώνονται από μια γραμμή εντολών, επεκτείνοντας ακόμη περισσότερο το περιβάλλον γραμμής εντολών των Windows XP. Αυτό το χαρακτηριστικό επιτρέπει τη χρήση script και τη διαχείριση σε μορφή ενός προς πολλά (one to many).

- Η βελτιωμένη λειτουργία προγραμματισμού εργασιών (Task Scheduler) επιτρέπει στους διαχειριστές να εκκινούν ένα σύνολο εργασιών σε μια συγκεκριμένη σειρά, διασφαλίζοντας ότι δεν λειτουργούν ταυτόχρονα και εκκινούν αυτόματα εργασίες ως επακόλουθο σε συμβάντα ή όταν ο υπολογιστής είναι σε αδράνεια. Τα στοιχεία σύνδεσης (credentials) που χρησιμοποιούνται για την εκκίνηση των εργασιών μπορούν πλέον να αποθηκεύονται στο Active Directory παρά στον τοπικό υπολογιστή ώστε να ενισχύουν την ασφάλεια των κωδικών πρόσβασης και να απλοποιούν τις υποχρεωτικές αλλαγές κωδικού πρόσβασης.

4.1.8.6 Δυνατότητα υποστήριξης

Τα Windows Vista έχουν σχεδιαστεί ώστε να μειώνουν τις δαπάνες υποστήριξης με τέσσερις βασικούς τρόπους:

- **Μείωση του αριθμού περιστατικών.** Χαρακτηριστικά των Windows Vista, όπως η **Προστασία Πόρων των Windows (Windows Resource Protection)** και ο Έλεγχος Λογαριασμού Χρήστη (User Account Control), ενισχύουν την παραγωγικότητα των χρηστών, ενώ δεν τους επιτρέπουν να κάνουν αλλαγές στο σύστημα που θα μπορούσαν να επηρεάσουν την απόδοση του συστήματος. Επιπλέον, η ανάκαμψη βλαβών των Windows Vista επιλύει αυτόματα πολλά συνήθη προβλήματα.

- **Παροχή βοήθειας στους χρήστες.** Τα Windows Vista έχουν κατασκευαστεί για να βοηθούν τους χρήστες να επιλύουν μόνοι τους τα προβλήματα που προκύπτουν, μειώνοντας σημαντικά την ανάγκη για υποστήριξη από τους διαχειριστές IT ή τους επαγγελματίες των κέντρων τεχνικής υποστήριξης. Το χαρακτηριστικό Υποστήριξη Χρήστη (User Assistance) - η έκδοση των αρχείων βοήθειας των Windows Vista - παρέχει καλύτερες δυνατότητες αναζήτησης, είναι πιο κατανοητή για τους τελικούς χρήστες και μπορεί να προσαρμοστεί από το IT τμήμα.

- **Μείωση του χρόνου υποστήριξης.** Όταν εμφανίζονται προβλήματα, τα Windows Vista παρέχουν στους επαγγελματίες του τμήματος IT και του κέντρου υποστήριξης εργαλεία, αναλυτικά συμβάντα και μετρητές απόδοσης που τους διευκολύνουν να προσδιορίσουν τι έχει συμβεί και πώς να το διορθώσουν. Η ικανότητα ανίχνευσης βλαβών στους δίσκους και τη μνήμη επιτρέπει στους IT επαγγελματίες να αντικαθιστούν προληπτικά το υλικό πριν το πρόβλημα αποβεί καταστροφικό, επιτρέποντας την επίλυση του προβλήματος σε λίγα λεπτά.

- **Μείωση του κόστους υποστήριξης απομακρυσμένων χρηστών.** Το βελτιωμένο εργαλείο Απομακρυσμένης Υποστήριξης (Remote Assistance) των Windows Vista διευκολύνει και καθιστά πιο οικονομική τη συντήρηση υπολογιστών σε απομακρυσμένες τοποθεσίες. Για να μειώσετε τις δαπάνες εύρους ζώνης, η εξαιρετικά βελτιωμένη υπηρεσία Background Intelligent Transfer Service (BITS) επιτρέπει σε υπολογιστές ενός τοπικού δικτύου (LAN) να χρησιμοποιούν από κοινού ενημερώσεις απευθείας αντί να "κατεβάζουν" τα ίδια αρχεία επανειλημμένα σε δίκτυα ευρείας περιοχής (WANs).

4.1.9 Αξιοπιστία και Απόδοση

Τα Windows Vista , εκτός από την καλύτερη αξιοποίηση του σύγχρονου υλικού (hardware) , λειτουργούν ταχύτερα και πιο αξιόπιστα στους ίδιους υπολογιστές οι οποίοι παλιότερα διάθεταν Windows XP. Το λειτουργικό σύστημα είναι πιο αξιόπιστο και το χαρακτηριστικό Διαχείρισης Επανεκκίνησης (Restart Manager) περιορίζει τον αριθμό αναγκαίων επανεκκινήσεων του υπολογιστή . Οι εφαρμογές που λειτουργούν σε Windows Vista είναι επίσης πιο αξιόπιστες , επειδή μπορούν να ανακτήσουν τη λειτουργία από αδιέξοδες καταστάσεις ενώ η βελτιωμένη λειτουργία αναφοράς σφαλμάτων επιτρέπει στους προγραμματιστές να διορθώνουν κοινά προβλήματα . Τα Windows Vista μπορούν ακόμη να συμβάλλουν στην ανίχνευση και ην επαναφορά εσφαλμένων σκληρών δίσκων και μνήμης .

4.1.9.1 Αυτόματη Ανάκαμψη

Στα Windows XP και τα παλαιότερα λειτουργικά συστήματα , η διαδικασία ανάκαμψης μετά από μια αποτυχία του συστήματος απαιτούσε επανεκκίνηση του υπολογιστή από τον χρήστη. Με τα Windows Vista , οι περισσότερες αποτυχίες δεν γίνονται αντιληπτές από τους χρήστες , επειδή τα Windows Vista επανεκκινούν αυτόματα τις περισσότερες υπηρεσίες σε περίπτωση που αποτύχουν . Εάν κριθεί απαραίτητο , τα Windows Vista μπορούν αυτόματα να καλύψουν εξαρτήσεις υπηρεσιών και να επανεκκινήσουν πολλαπλές υπηρεσίες για την διατήρηση της αξιοπιστίας του λειτουργικού συστήματος . Επειδή οι χρήστες επανεκκινούσαν συχνά τον υπολογιστή τους για να επιλύσουν προβλήματα με αποτυχημένες υπηρεσίες , η αυτόματη ανάκτηση μειώνει , επίσης, τον αριθμό των επανεκκινήσεων.

4.1.9.2 Ενσωματωμένοι Διαγνωστικοί Έλεγχοι

Τα Windows Vista μπορούν να διαγνώσουν και να αποκαταστήσουν αυτόματα αρκετά συνήθη προβλήματα . Για παράδειγμα , το χαρακτηριστικό **Windows Disk Diagnostics** ανιχνεύει προληπτικά επικείμενες αποτυχίες δίσκου και μπορεί να ενημερώσει το κέντρο υποστήριξης ώστε να αντικαταστήσει τον εσφαλμένο σκληρό δίσκο πριν προκύψει ολοκληρωτική βλάβη. Τα Windows Vista καθοδηγούν τους διαχειριστές μέσω της διαδικασίας δημιουργίας αντιγράφων ασφαλείας των δεδομένων τους , επομένως ο σκληρός δίσκος μπορεί να αντικατασταθεί χωρίς να χαθούν τα δεδομένα.
Τα Windows Vista συμπεριλαμβάνουν , επίσης, διαγνωστικό έλεγχο μνήμης , που βοηθά τους διαχειριστές να εντοπίζουν προβλήματα αξιόπιστης μνήμης.

Παλιότερα , ο διαγνωστικός έλεγχος μνήμης ήταν διαθέσιμος μόνο ως download και ήταν δύσχρηστος για πολλούς IT επαγγελματίες. Στα Windows Vista ,εάν **η Λειτουργία Σφαλμάτων των Windows (Windows Error Reporting - WER) ή η Λειτουργία Online Ανάλυσης Σφαλμάτων της Microsoft (Microsoft Online Crash Analysis - MOCA)** προσδιορίζει ότι μπορεί να προκληθεί αποτυχία λόγω βλάβη της μνήμης , τα Windows Vista ζητούν από το χρήστη να εκτελέσει διαγνωστικό έλεγχο μνήμης χωρίς να απαιτείται πρόσθετη λήψη ή ξεχωριστό CD εκκίνησης . Εάν ο διαγνωστικός έλεγχος μνήμης εντοπίσει πρόβλημα μνήμης , τα Windows Vista μπορούν να αποτρέψουν την χρήση του προσβεβλημένου τμήματος της μνήμης προκειμένου να γίνεται σωστά η επανεκκίνηση του λειτουργικού συστήματος και να αποτρέπονται οι βλάβες των εφαρμογών .

Κατά την εκκίνηση , τα Windows Vista παρέχουν μια απλή και εύκολα κατανοητή αναφορά που περιγράφει αναλυτικά το πρόβλημα . Τα Windows Vista περιλαμβάνουν επίσης το χαρακτηριστικό **Network Diagnostics Framework (NDF)** . Το NDF παρέχει στους χρήστες προηγμένα μέσα που βοηθούν στην επίλυση προβλημάτων για ζητήματα που σχετίζονται με τον δίκτυο. Όταν ο χρήστης δεν μπορεί να συνδεθεί σε ένα πόρο δικτύου , παρουσιάζονται σαφείς επιλογές επανόρθωσης και όχι δυσνόητα μηνύματα σφαλμάτων. Εάν τα Windows Vista μπορούν να επανορθώσουν το πρόβλημα αυτόματα , θα το κάνουν , διαφορετικά ο χρήστης κατευθύνεται μέσα από απλά βήματα για να διορθώσει το πρόβλημα χωρίς να χρειάζεται να καλέσει τεχνική υποστήριξη.

4.1.9.3 Startup Repair Tool – Εργαλείο Αποκατάστασης Εκκίνησης

Τα Windows Vista περιλαμβάνουν το **Εργαλείο Αποκατάστασης Εκκίνησης (Startup Repair Tool –StR)** που αποκαθιστά πολλά συνήθη προβλήματα και επιτρέπει στου τελικούς χρήστες και τους IT επαγγελματίες να διαγιγνώσκουν και να αποκαθιστούν γρήγορα πιο περίπλοκα προβλήματα εκκίνησης. Όταν ανιχνεύεται μια αποτυχία , το σύστημα απευθύνεται στο StR. . Μόλις τεθεί σε λειτουργία , το StR εκτελεί διαγνωστικό έλεγχο για να προσδιορίσει την αιτία της αποτυχίας εκκίνησης. Το StR αναλύει ακόμη και τα αρχεία συμβάντων , επομένως δεν χρειάζεται να το κάνει ο χρήστης. Μόλις το StR εντοπίσει την αιτία της αποτυχίας , επιχειρεί να αποκαταστήσει το πρόβλημα αυτόματα. Ολόκληρη η διαδικασία απαιτεί μικρή έως και μηδαμινή παρέμβαση του χρήστη . Το StR μπορεί να αποκαταστήσει αυτόματα προβλήματα, όπως:

- Ασύρματα προγράμματα οδήγησης.
- Απώλεια ή αλλοίωση ρυθμίσεων διαμόρφωσης εκκίνησης (startup configuration settings)
- Αλλοιωμένα δεδομένα στον δίσκο.

Αφού αποκατασταθεί το λειτουργικό σύστημα , τα Windows Vista ενημερώνουν το χρήστη για τις επανορθώσεις και παρέχουν αρχεία καταγραφής συμβάντων έτσι ώστε οι IT επαγγελματίες να μπορούν να προσδιορίσουν επακριβώς ποια βήματα εκτέλεσε το StR. Το StR περιλαμβάνει , επίσης , εργαλεία που βοηθούν τους IT επαγγελματίες να αντιμετωπίζουν χειροκίνητα τα προβλήματα εκκίνησης . Το StR περιορίζει τις κλήσεις για τεχνική υποστήριξη που σχετίζονται με προβλήματα εκκίνησης και όταν οι χρήστες χρειάζονται όντως βοήθεια , το StR τους βοηθά να λύσουν γρήγορα το πρόβλημα.

4.1.9.4 Αξιοπιστία Εφαρμογών

Τα Windows Vista είναι κατασκευασμένα ώστε να μειώνουν τη συχνότητα και την επίδραση των διάφορων διαταράξεων κατά τη λειτουργία , προς τον τελικό χρήστη . Περιλαμβάνουν διορθωτικά προγράμματα για γνωστές περιπτώσεις βλαβών και διακοπών λειτουργίας και βελτιωμένα όργανα που παρέχουν σημαντικότερη δυνατότητα ανίχνευσης των αιτιών όταν το σύστημα δεν ανταποκρίνεται.

Τα Windows Vista προσφέρουν βελτιωμένη αξιοπιστία εφαρμογών από την πρώτη ημέρα της εγκατάστασής τους σε μια επιχείρηση και οι νέες δυνατότητες αναφοράς σφαλμάτων θα αυξηθούν ακόμη περισσότερο για τις εφαρμογές με το χρόνο. Στις παλαιότερες εκδόσεις των Windows , οι προγραμματιστές αντιμετώπιζαν με δυσκολία τις διακοπές λειτουργίας των εφαρμογών επειδή η λειτουργία αναφοράς σφαλμάτων παρείχε περιορισμένες ή μηδαμινές πληροφορίες σχετικά με τις διακοπές λειτουργίας . Τα Windows Vista βελτιώνουν τη λειτουργία αναφοράς σφαλμάτων και δίνουν στους προγραμματιστές τις πληροφορίες που χρειάζονται για τον εντοπισμό της βασικής αιτίας των προβλημάτων . Αυτό επιτρέπει την συνεχή βελτίωση στο θέμα της αξιοπιστίας .

4.1.9.5 Βελτιώσεις απόδοσης

Τα Windows Vista προσφέρουν βελτιωμένη απόδοση και ανταπόκριση σε σύγκριση με τα Windows XP. Για παράδειγμα , τα Windows Vista μπορούν να ανιχνεύσουν αυτόματα προβλήματα που σχετίζονται με υψηλούς χρόνους εκκίνησης ή μη ανταπόκριση του περιβάλλοντος εργασίας και προσθέτουν ένα συμβάν στο αρχείο καταγραφής συμβάντων το οποίο περιγράφει την κατάσταση και πιθανόν ενημερώνει για την κύρια αιτία του προβλήματος απόδοσης . Οι διαχειριστές μπορούν να χρησιμοποιούν αυτές τις πληροφορίες για να αντιμετωπίζουν προβλήματα κατά περίπτωση ή για να συγκεντρώνουν τα δεδομένα του αρχείου καταγραφής συμβάντων με ένα εργαλείο , όπως το **Microsoft Operations Manager (MOM)** για την ανάλυση της απόδοσης σε ολόκληρο τον οργανισμό.

Το TCP/IP stack επόμενης γενιάς ανιχνεύει αυτόματα το περιβάλλον δικτύου και προσαρμόζει τις κύριες ρυθμίσεις απόδοσης, όπως το TCP receive windows . Ο βελτιωμένος αυτόματος συντονισμός και διαμόρφωση του stack περιορίζει την ανάγκη για χειροκίνητη διαμόρφωση των ρυθμίσεων TCP/IP . Επιτρέπει ταχύτερες δικτυακές μεταφορές , πιο έξυπνη χρήση του εύρους ζώνης και λιγότερες αναμεταδόσεις απολεσθέντων δεδομένων στο δίκτυο . Αυτό μπορεί να οδηγήσει σε σημαντική μείωση μέσα στο χρόνο που απαιτείται για τη μεταφορά ενός μεγάλου αρχείου ή για τη δημιουργία αντιγράφων ασφαλείας σκληρού δίσκου στο δίκτυο.

4.1.9.6 Εγκατάσταση

Η εγκατάσταση ενός νέου λειτουργικού συστήματος σε μια επιχείρηση είναι ένα δύσκολο έργο, αλλά η μαζική εγκατάσταση με χρήση πιστών αντιγράφων (images) των Windows Vista καθιστά τη διαδικασία εξαιρετικά αποτελεσματική. Τα πιστά αντίγραφα είναι ο πιο αξιόπιστος και γρήγορος τρόπος εγκατάστασης ενός λειτουργικού συστήματος αλλά δεν αποτελούν παραδοσιακά μέρος της τυπικής εγκατάστασης του λειτουργικού συστήματος των Windows αλλά απαιτούν πρόσθετο λογισμικό και πολλές ώρες εργασίας για συντήρηση . Για να περιορίσει την πολυπλοκότητα της διαδικασίας μαζικής εγκατάστασης , η Microsoft στήριξε την εγκατάσταση των Windows Vista στην τεχνολογία δημιουργίας αντιγράφων των αρχείων ενός δίσκου , που λέγεται **Windows Imaging (WIM)**. Επιπλέον , τμηματοποίησε τα Windows Vista ώστε να διευκολύνει την προσαρμογή και την ανάπτυξη των πιστών αντιγράφων και προχώρησε σε σημαντικές βελτιώσεις όσον αφορά την εγκατάσταση , στον πυρήνα του λειτουργικού συστήματος.

4.1.9.7 Modularization (Τμηματοποίηση)

Τα Windows Vista έχουν τμηματοποιηθεί σε υπομονάδες, γεγονός που καθιστά ευκολότερη την προσαρμογή τους. Κατά την προετοιμασία της διανομής των Windows Vista σε έναν οργανισμό, οι IT επαγγελματίες προσαρμόζουν και προσθέτουν προαιρετικά στοιχεία για να τα διανείμουν σε ένα συγκεκριμένο σύνολο υπολογιστών. Οι γλώσσες, για παράδειγμα, είναι συστατικά στοιχεία, επομένως η Αγγλική γλώσσα μπορεί να διανεμηθεί σε ένα σύνολο υπολογιστών, ενώ η Γαλλική, η Γερμανική και η Ισπανική να διανεμηθεί σε διαφορετικό σύνολο. Τα προγράμματα οδήγησης και οι ενημερώσεις είναι επίσης συστατικά στοιχεία, που διευκολύνουν την ενημέρωση των πιστών αντιγράφων, καθώς αλλάζουν οι απαιτήσεις του υλικού και του λογισμικού.

4.1.9.8 Windows Imaging

Το WIM είναι μια μορφή πιστών αντιγράφων βάσει αρχείων (file - based images), που παρέχει σημαντικά οφέλη σε σύγκριση με τις συνηθέστερες μορφές πιστών αντιγράφων, που βασίζονται σε τομείς (sector - based images). Η μορφή πιστών αντιγράφων WIM δεν εξαρτάται από το υλικό (hardware) και σας επιτρέπει να διατηρήσετε μόνο ένα πιστό αντίγραφο για πολλαπλές διαμορφώσεις υλικού. Το WIM μπορεί, επίσης, να αποθηκεύσει πολλαπλά πιστά αντίγραφα μέσα σε ένα αρχείο πιστών αντιγράφων, διευκολύνοντας τη διαχείριση πιστών αντιγράφων και εξοικονομώντας χώρο στο δίσκο αποθηκεύοντας μόνο ένα αντίγραφο για κάθε αρχείο.

Για παράδειγμα, μπορείτε να αποθηκεύσετε δύο πιστά αντίγραφα σε ένα αρχείο WIM - ένα πιστό αντίγραφο που περιέχει μόνο το λειτουργικό σύστημα των Windows Vista και ένα δεύτερο πιστό αντίγραφο που περιέχει επίσης και τις απολύτως βασικές (core) εφαρμογές. Η μορφή WIM μειώνει σημαντικά τα μεγέθη του αρχείου πιστών αντιγράφων χρησιμοποιώντας συμπιεσμένη μορφή αρχείου και τεχνικές αποθήκευσης μίας παρουσίας (instance). (Το αρχείο πιστών αντιγράφων περιέχει μόνο ένα φυσικό αντίγραφο ενός αρχείου για κάθε παρουσία στο αρχείο πιστών αντιγράφων, που μειώνει σημαντικά το μέγεθος των αρχείων πιστών αντιγράφων που περιέχουν πολλαπλά πιστά αντίγραφα).

Η διατήρηση των πιστών αντιγράφων WIM είναι εύκολη, επειδή τα προγράμματα οδήγησης, οι ενημερώσεις και πολλά άλλα συστατικά στοιχεία των Windows μπορούν να προστεθούν και να καταργηθούν offline χωρίς καν να γίνεται εκκίνηση του πιστού αντιγράφου του λειτουργικού συστήματος. Τα Windows Vista περιλαμβάνουν εργαλεία που τροποποιούν απευθείας τα πιστά αντίγραφα προκειμένου να αλλάξουν τις γενικές και περιφερειακές ρυθμίσεις, να εφαρμόσουν ενημερώσεις λειτουργικού συστήματος, να προσθέσουν προγράμματα περιήγησης και να εγκαταστήσουν ενημερώσεις.
Αυτό το χαρακτηριστικό εξοικονομεί ώρες εργασίας κατά τη συντήρηση και διατήρηση ενημερωμένων πιστών αντιγράφων , επειδή δεν υπάρχει ανάγκη να γίνει εκκίνηση του πιστού αντιγράφου για να γίνουν οι αλλαγές διαμόρφωσης.
Επίσης, η μορφή πιστών αντιγράφων WIM επιτρέπει την μη καταστροφική εγκατάσταση (non-destructive deployment). Αυτό σημαίνει ότι στον δίσκο στον οποίο γίνεται η εφαρμογή του πιστό αντίγραφο, μπορούν να αφεθούν δεδομένα καθώς η εφαρμογή του πιστού αντιγράφου δεν διαγράφει τα υπάρχοντα περιεχόμενα του δίσκου.
Είτε η τμηματοποίηση είτε μόνο το WIM μπορούν να απλοποιήσουν σημαντικά την ανάπτυξη, αλλά σε συνδυασμό αποτελούν την επανάσταση στην εγκατάσταση client λειτουργικών συστημάτων. Με άλλα λόγια, ο συνδυασμός και των δύο τεχνολογιών παρέχει ένα σημαντικότερο πλεονέκτημα απ' ότι θα μπορούσε να προσφέρει καθεμία τεχνολογία ξεχωριστά. Πιο συγκεκριμένα, οι δύο τεχνολογίες μειώνουν σημαντικά τον αριθμό των πιστών αντιγράφων του λειτουργικού συστήματος που πρέπει να διατηρηθούν. Με άλλα λόγια, τα εταιρικά τμήματα IT, που προηγουμένως διατηρούσαν διαφορετικά πιστά αντίγραφα για κάθε γλώσσα και τύπο υπολογιστή, μπορούν πιθανόν να χρησιμοποιήσουν μόνο ένα ή δύο πιστά αντίγραφα των Windows Vista, απαλλάσσοντας έτσι το προσωπικό για να αφοσιωθεί σε άλλες προτεραιότητες.

4.1.9.9 Non-destructive Imaging (Μη Καταστροφική Δημιουργία Πιστών Αντιγράφων Σκληρού Δίσκου)

Σε προηγούμενες εκδόσεις των Windows, η δημιουργία πιστών αντιγράφων σκληρού δίσκου (imaging) μπορούσε να χρησιμοποιηθεί μόνο για νέες εγκαταστάσεις των Windows, καθώς η ανάπτυξη ενός πιστού αντιγράφου θα μπορούσε να αντιγράψει το σκληρό δίσκο του υπολογιστή. Για να αναβαθμίσουν τον υπολογιστή ενός χρήστη, οι IT επαγγελματίες έπρεπε να αντιγράψουν τα αρχεία και τις ρυθμίσεις του χρήστη σε έναν διαφορετικό υπολογιστή και κατόπιν να

επαναφέρουν τα αρχεία και τις ρυθμίσεις μετά την ανάπτυξη του πιστού αντιγράφου. Τα Windows Vista περιλαμβάνουν τη μη καταστροφική δημιουργία πιστών αντιγράφων στο σκληρό δίσκο μέσω πιστών αντιγράφων WIM, στα οποία γίνεται αντιγραφή των αρχείων και των ρυθμίσεων σε δεσμευμένο τμήμα του σκληρού δίσκου του υπολογιστή πριν από την ανάπτυξη του πιστού αντιγράφου των Windows Vista. Αφού το πιστό αντίγραφο των Windows Vista εγκατασταθεί, τα Windows Vista μετεγκαθιστούν τα αρχεία και τις ρυθμίσεις και κατόπιν επαναφέρουν το τμήμα του σκληρού δίσκου του υπολογιστή που είχε δεσμευτεί. Γενικά, η μετεγκατάσταση στα Windows Vista είναι πολύ πιο αξιόπιστη από τη μετεγκατάσταση στα Windows XP.

4.1.9.10 Unattended Installations (Εγκαταστάσεις Χωρίς Παρακολούθηση)

Τα περισσότερα διαχειριστικά εργαλεία των Windows Vista, όπως το **Windows System Image Manager** και το **Microsoft Windows User State Migration Tool (USMT)**, μπορούν να ελεγχθούν από μια γραμμή εντολών ή ένα script. Με αυτές τις λειτουργίες ο χρήστης μπορεί να εξοικονομήσει χρόνο όταν πρέπει να εκτελέσει επανειλημμένα τις ίδιες ή παρόμοιες ενέργειες. Τα τμήματα IT που δεν χρησιμοποιούν script μπορούν επίσης να εξοικονομούν χρόνο διαμορφώνοντας τις ρυθμίσεις της εγκατάστασης χωρίς παρακολούθηση τροποποιώντας ένα αρχείο, το Unattended.xml. Τα Windows Vista περιλαμβάνουν γραφικά εργαλεία που διευκολύνουν τη διαμόρφωση εγκατάστασης χωρίς παρακολούθηση, χωρίς να απαιτείται τροποποίηση του αρχείου χειροκίνητα. Επειδή τα αρχεία Extensible Mark up Language (XML) βασίζονται σε κείμενο, είναι δυνατό να τροποποιηθούν χειροκίνητα ή προγραμματιστικά με χρήση ενός script.

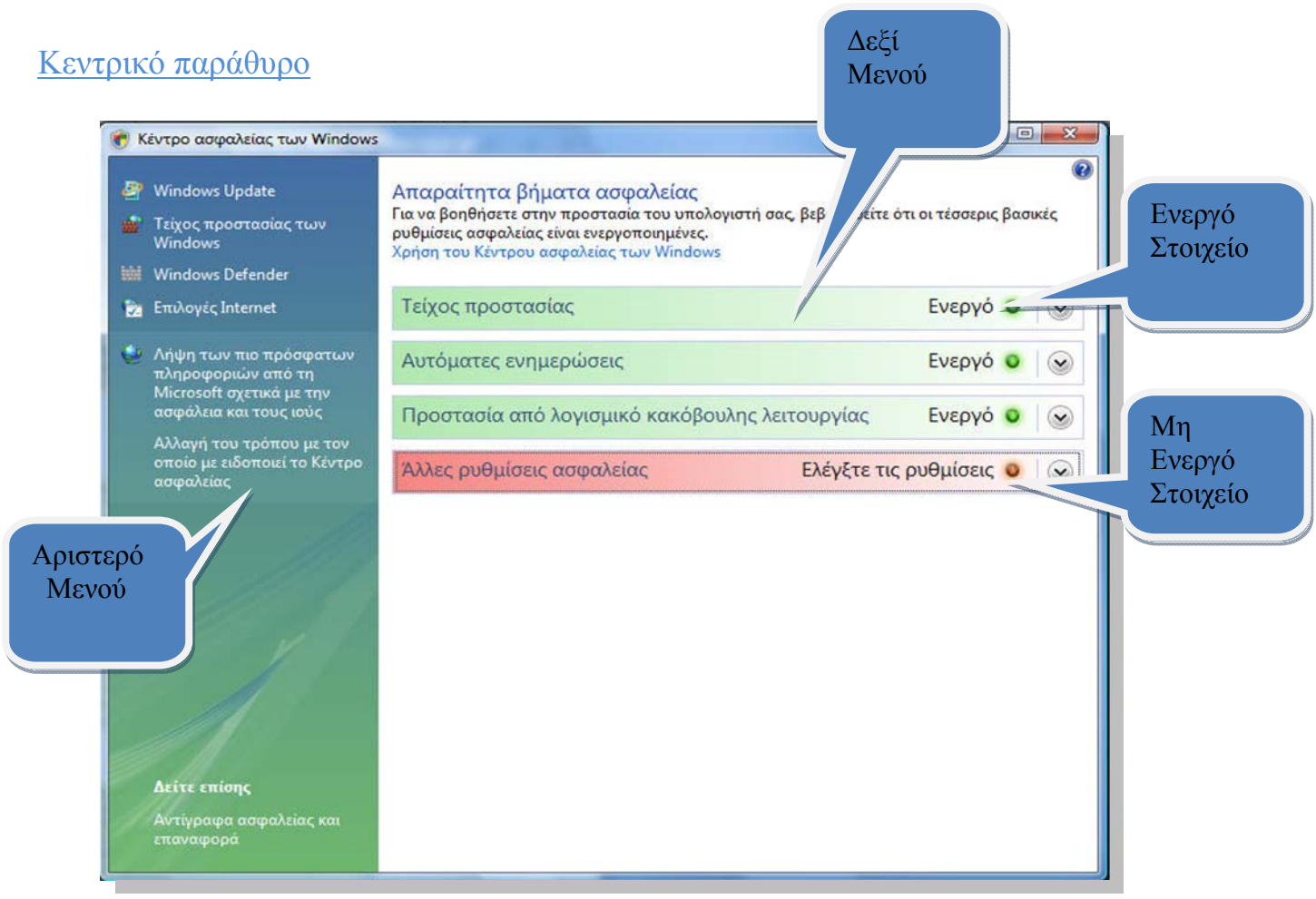
5 ΚΕΝΤΡΟ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ WINDOWS VISTA

Τα Windows Vista διαθέτουν ένα ανεπτυγμένο κέντρο ασφαλείας, που συμβάλλει στην βελτίωση του υπολογιστή .
Το κέντρο ασφαλείας λειτουργεί ως ρυθμιστής και ως επόπτης των επιμέρους στοιχείων ασφαλείας που διαθέτουν τα Windows Vista όπως παραδείγματος χάριν του Τείχους Προστασίας, των Αυτόματων Ρυθμίσεων, των Ρυθμίσεων Λογισμικού Προστασίας από λογισμικό κακόβουλης, των Ρυθμίσεων του Internet, των Ρυθμίσεων Ελέγχου Λογαριασμού Χρήστη κ.α.

Μέσω λοιπόν αυτών των στοιχείων που προαναφέρθηκαν, πραγματοποιούνται διάφοροι έλεγχοι ασφάλειας στο σύστημά μας . Σε περίπτωση τώρα που εντοπιστεί οποιοδήποτε πρόβλημα πχ το πρόγραμμα προστασίας μας από ιούς να είναι πεπαλαιωμένο, ή χειρότερα η ανίχνευση ενός ιού το Κέντρο Προστασίας είναι υπεύθυνο να μας ειδοποιήσει άμεσα μέσω διαφόρων μηνυμάτων πχ να μας εμφανίσει κάποιο εικονίδιο ειδοποίησης περιοχή ειδοποιήσεων . Πατώντας στην συνέχεια πάνω στην περιοχή ειδοποιήσεων , εμφανίζεται συνοπτική περιγραφή του προβλήματος που έχει εντοπιστεί .
Προκειμένου τώρα να μπούμε στο Κέντρο Ασφαλείας του συστήματος μας πρέπει να μπούμε στον Πίνακα Ελέγχου και από κει πατώντας στο εικονίδιο με την ασπίδα , παρατηρώντας το κεντρικό παράθυρο του Κέντρου Ασφαλείας , διακρίνουμε κάποια στοιχεία μέσω των οποίων ,μπορούμε να ρυθμίσουμε κάποιες επιμέρους παραμέτρους του

5.1 Περιγραφή του Κέντρου Ασφάλειας των Windows Vista

Κεντρικό παράθυρο



Εικόνα 2: Παράθυρο Κέντρου Ασφαλείας των Windows.

Στο *αριστερού μενού* βρίσκονται οι συντομεύσεις των στοιχείων:

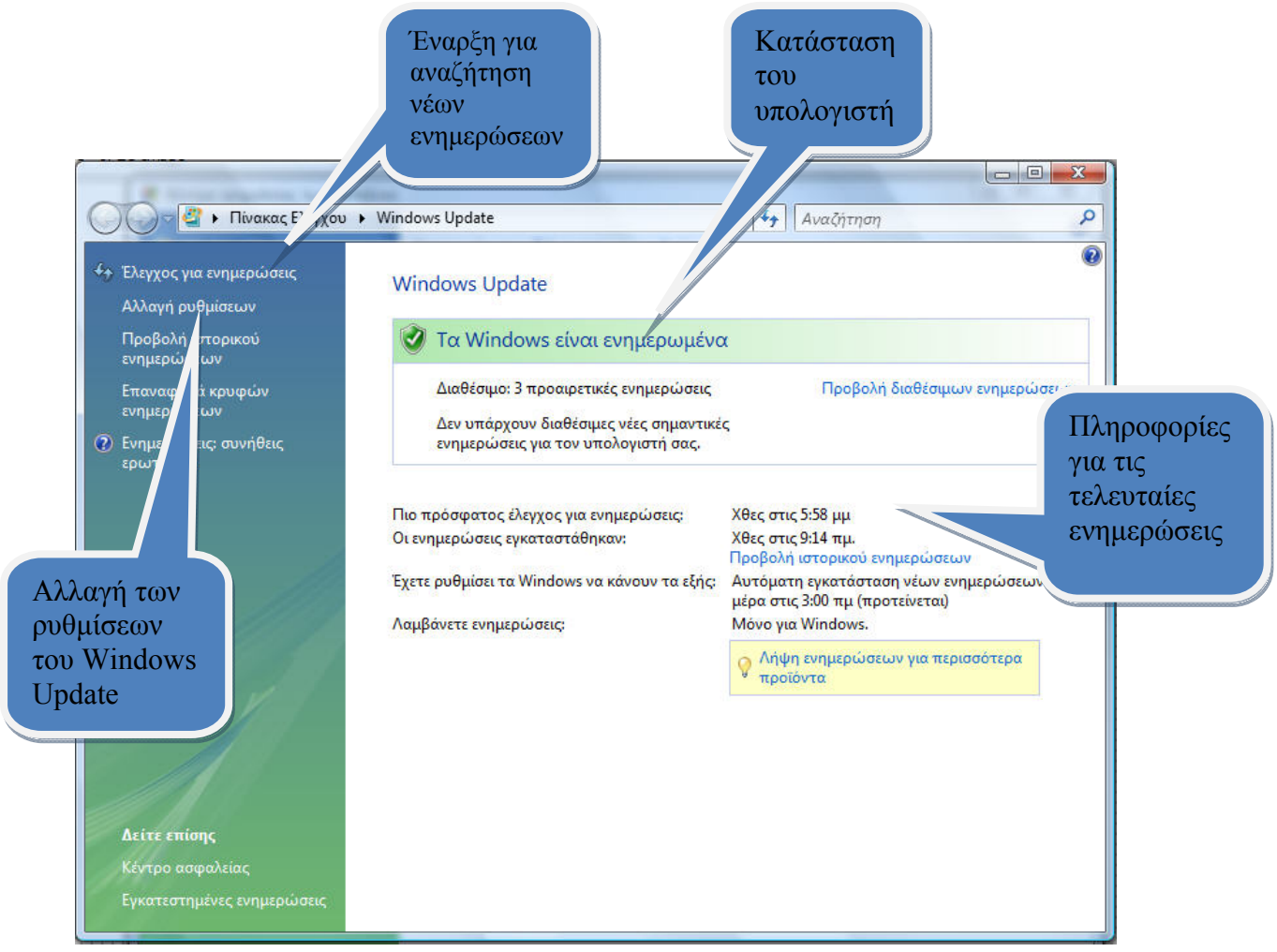
- Windows Update.
- Τείχος προστασίας των Windows.
- Windows Defender.
- Επιλογές Internet.
- Λήψη των πιο πρόσφατων πληροφοριών από την Microsoft σχετικά με την ασφάλεια και τους ιούς.
- Αλλαγή του τρόπου με τον οποίο με ειδοποιεί το Κέντρο ασφαλείας .

Στο *δεξί μενού* γίνεται αναφορά ποια στοιχεία είναι ενεργά και ποια ανενεργά .
Με πράσινο χρώμα αναφέρονται τα ενεργά στοιχεία με κόκκινο χρώμα τα μη ενεργά στοιχεία ή τα ημιενεργά στοιχεία.
Εκτεταμένη περιγραφή του καθενός θα γίνει στις παραγράφους που ακολουθούν .

5.1.1 Αυτόματες Ενημερώσεις (Windows Update).

Το πρώτο από τα στοιχεία ασφάλειας που αναγράφονται στο αριστερό μενού είναι οι **Αυτόματες ενημερώσεις (Windows Update) .**
Το στοιχείο αυτό επηρεάζει σε μεγάλο βαθμό την ασφάλεια του συστήματος , και αυτό γιατί όσα προγράμματα ασφαλείας και αν χρησιμοποιούμε αν δεν είναι ενημερωμένα για τις νέες απειλές ,δεν θα μπορέσουν να μας προστατέψουν.
Θα μπορούσαμε λοιπόν να πούμε ότι όσο λιγότερο ενημερωμένο είναι ένα σύστημα τόσο περισσότερο ευάλωτο είναι .
Το στοιχείο αυτό ξεκινάει κάνοντας μια περίληψη της κατάστασης του υπολογιστή .
Συγκεκριμένα μας πληροφορεί για το αν το σύστημά μας έχει λάβει ή όχι τις πιο πρόσφατες ενημερώσεις, καθώς και για το αν υπάρχουν άλλες προαιρετικές .

Κεντρικό παράθυρο του Windows Update

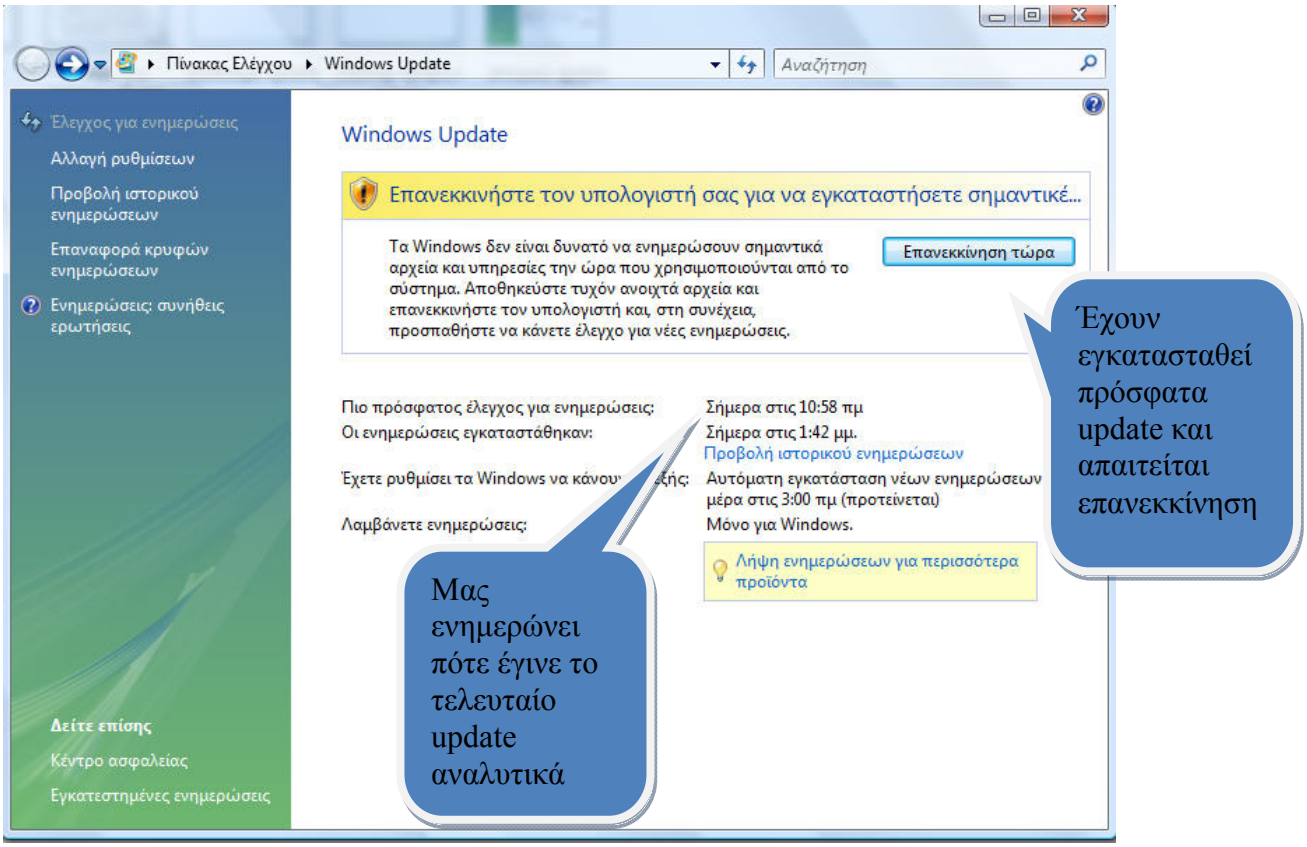


Εικόνα 3: Παράθυρο του Windows Update.

Αναλυτικά στο αριστερό μενού υπάρχουν οι ακόλουθες επιλογές :

5.1.1.1 Έλεγχος ενημερώσεων .

Γίνετε εκκίνηση διαδικασίας εύρεσης νέων ενημερώσεων επειγόντων ή προαιρετικών .Όταν ολοκληρωθεί και εφόσον εγκαταστήσουμε έστω και μια νέα ενημέρωση στο σύστημά μας , απαιτείται επανεκκίνηση προκειμένου να εφαρμοστούν σωστά οι νέες ρυθμίσεις.

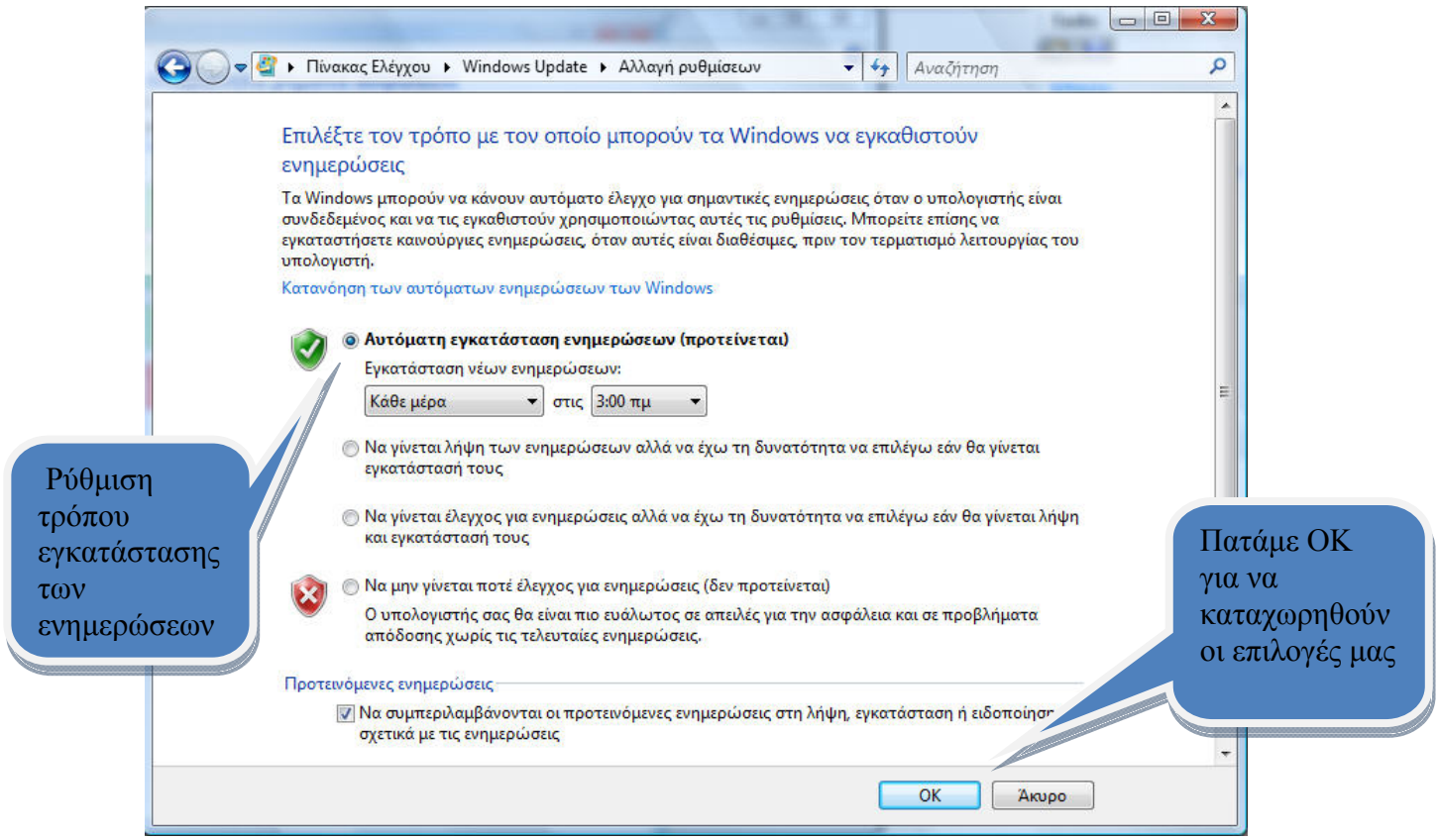


Εικόνα 4: Παράθυρο ελέγχου για ενημερώσεις των Windows

.

5.1.1.2 Αλλαγή ρυθμίσεων :

Εδώ επιλέγουμε αν η διαδικασία του ελέγχου και της εγκατάστασης θα είναι αυτόματη η χειροκίνητη .

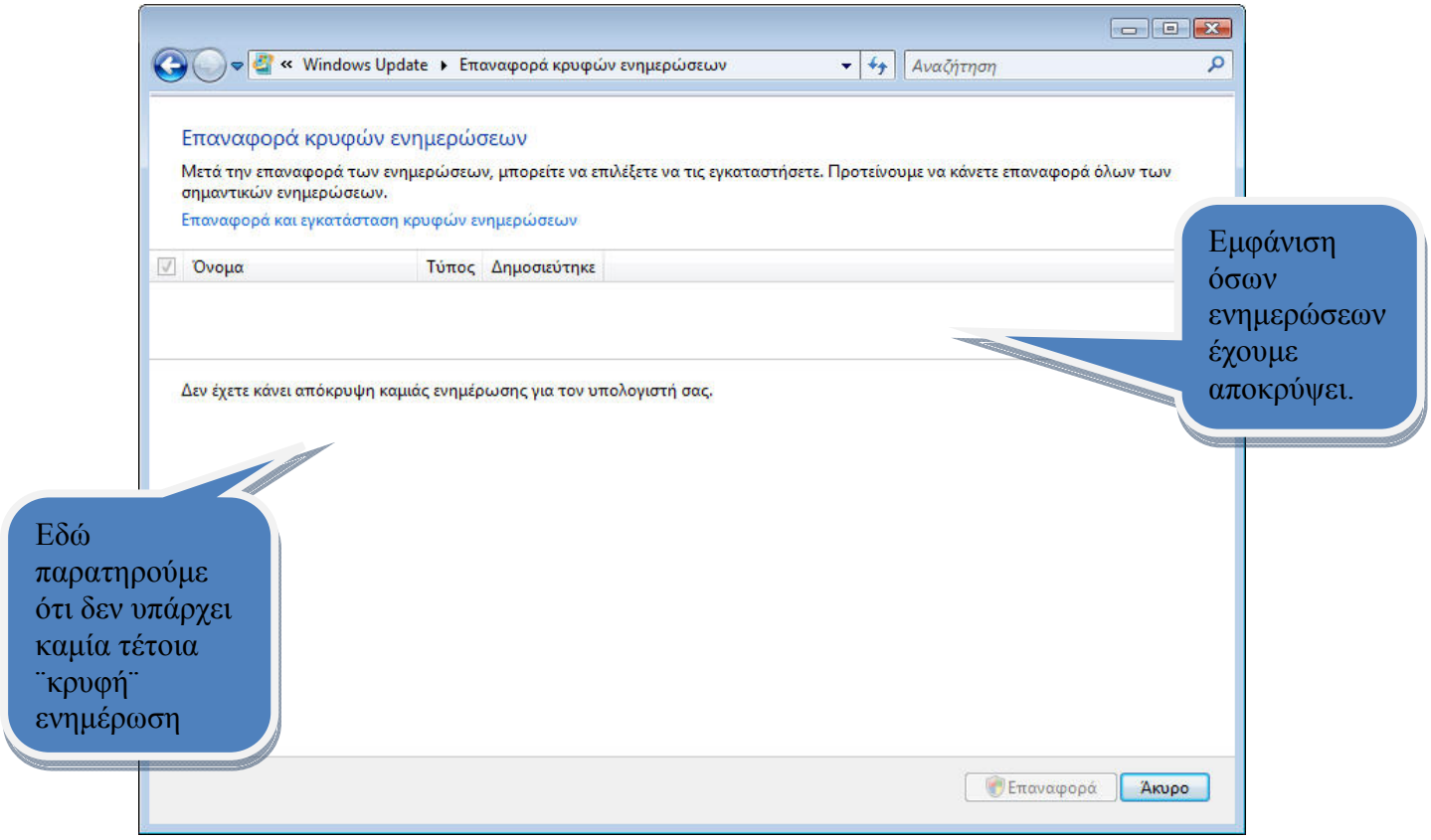


Εικόνα 5: Παράθυρο αλλαγή ρυθμίσεων του Windows Update.

5.1.1.3 Επαναφορά κρυφών ενημερώσεων

Στο παράθυρο αυτό εμφανίζονται όλες οι ενημερώσεις τις οποίες έχουμε ¨αποκρύψει¨. Με τον όρο αποκρύψει εννοούμε ότι ενώ οι ενημερώσεις αυτές ήταν διαθέσιμες για τον υπολογιστή μας , εμείς προτιμήσαμε να τις αγνοήσουμε για διάφορους λόγους , είτε γιατί δεν μας ενδιέφερε το περιεχόμενό τους, είτε γατί αποφασίσαμε να τις εγκαταστήσουμε αργότερα σε κάποια άλλη χρονική στιγμή .

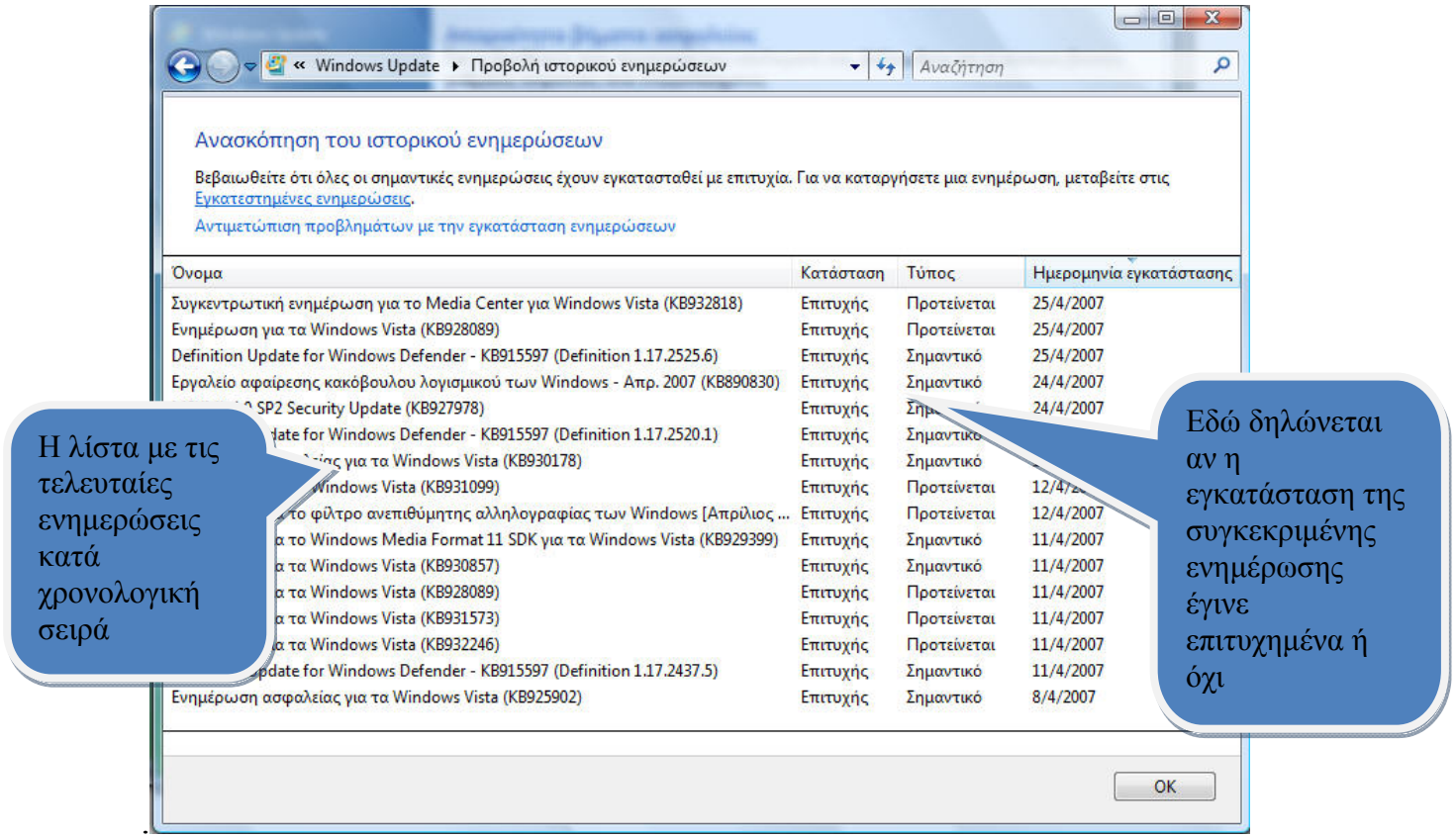
Εντούτοις , μέσω του παραθύρου αυτού έχουμε την δυνατότητα να τις επαναφέρουμε στο προσκήνιο ανά πάσα στιγμή ,με σκοπό την εγκατάσταση τους .



Εικόνα 6 : Παράθυρο Επαναφορά κρυφών ενημερώσεων του Windows Update.

5.1.1.4 Προβολή ιστορικού ενημερώσεων :

Εμφανίζεται ανασκόπηση του ιστορικού ενημερώσεων . Αναλυτικά εμφανίζεται ημερομηνία , ώρα , είδος και ονομασία της ενημέρωσης που έχουμε κατεβάσει και αποθηκεύσει στον σύστημα μας

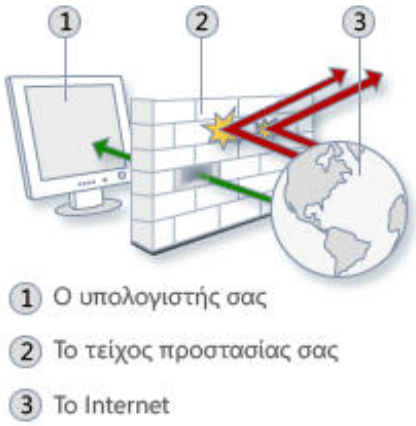


Εικόνα 7 : Παράθυρο προβολή ιστορικού ενημερώσεων τουWindows Update.

5.1.2 Τείχος προστασίας των Windows Vista - Firewall Windows.

Το Windows Firewall αποτελεί ένα από τα κυριότερα μέσα ασφάλειας του υπολογιστή μας . Είναι ένα κομμάτι του λογισμικού που ελέγχει τις πληροφορίες που προέρχονται από το Internet ή από ένα δίκτυο , και στην συνέχεια είτε τις αποκλείει είτε τους επιτρέπει να περάσουν στον υπολογιστή μας ανάλογα με τις ρυθμίσεις που του έχουμε θέσει. Αποτρέπει την επικοινωνία σε όσα προγράμματα θεωρεί επικίνδυνα , κακόβουλα ή βλαβερά και προστατεύει τον υπολογιστή από εξωτερικές επιθέσεις . Πλέον , χρήστες που χρησιμοποιούν το διαδίκτυο , είναι παραπάνω κι από απαραίτητο να χρησιμοποιούν Firewall.

Το Firewall αποτελεί την πρώτη γραμμή προστασίας του υπολογιστή και μπορεί να μας προστατεύσει από πολλών ειδών κακόβουλα λογισμικά.



Εικόνα 8 : Τρόπος λειτουργίας του Windows Firewall

Τα Windows Vista, συνοδεύονται από μια ανανεωμένη έκδοση του Firewall, η οποία εκτός από τις παλιές δυνατότητες που είχαμε στα Windows XP, διαθέτει επιπλέον μια πρόσθετη δυνατότητα, τον **έλεγχο πρόσβασης στο δίκτυο** , ακόμα και των εφαρμογών που εκτελούνται στον υπολογιστή μας. Ακόμη το Firewall , στα Windows Vista είναι κατάλληλα ρυθμισμένο έτσι ώστε να ενεργοποιείται με την έναρξη των Windows . Βασικό μέλημα των κατασκευαστών ήταν

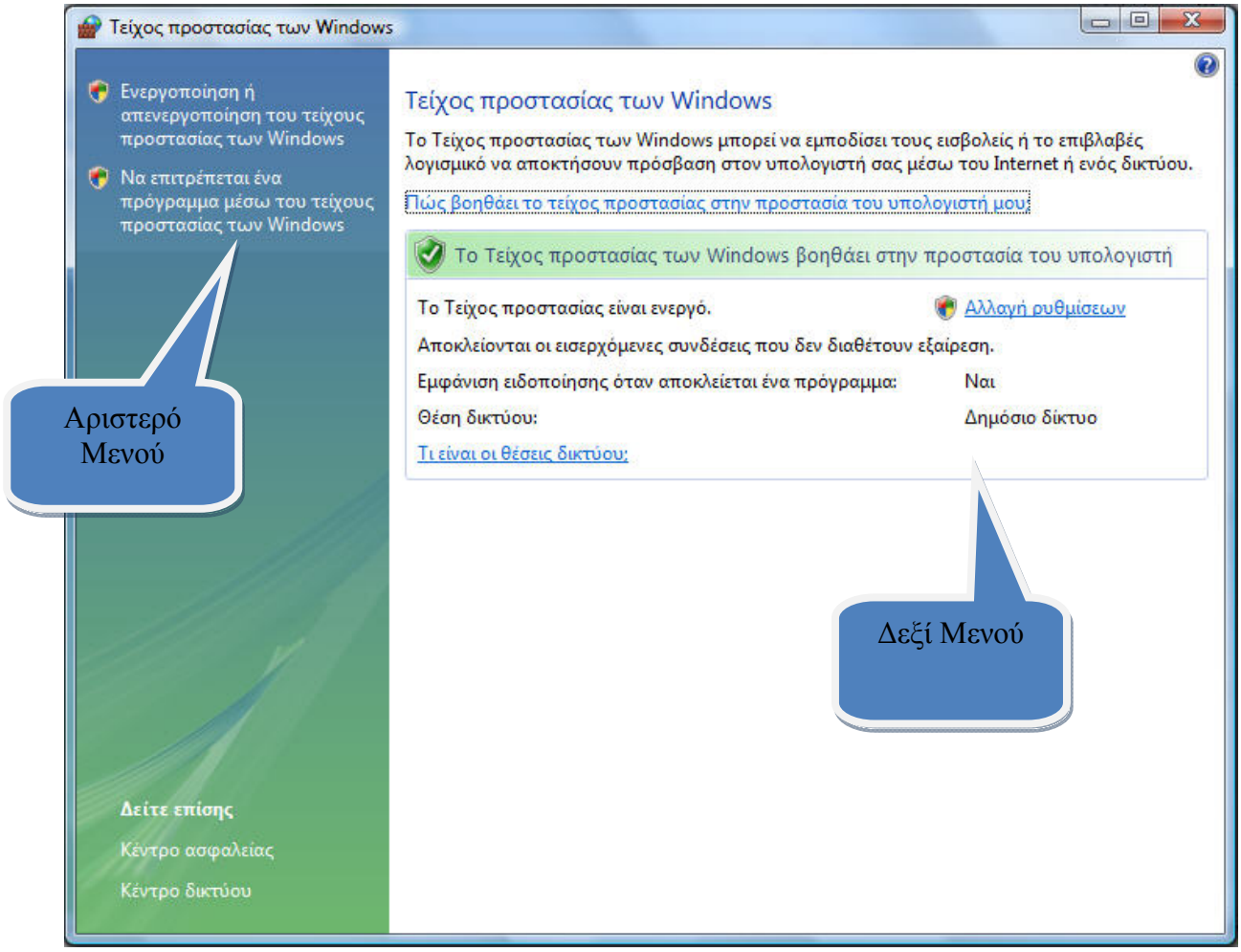
να δημιουργήσουν ένα Firewall το οποίο να είναι εύχρηστο προς τους χρήστες και να προσαρμόζεται απλά και γρήγορα ανάλογα με τις ανάγκες των χρηστών .

Το νέο Firewall των Windows Vista όπως προαναφέραμε διαθέτει μια νέα λειτουργία , τον έλεγχο πρόσβασης στο δίκτυο. Αναλυτικά ενώ το παλιό μας firewall απαγόρευε κάθε μη εξουσιοδοτημένη σύνδεση που προέρχεται από ξένα μηχανήματα, τώρα το νέο firewall ελέγχει και τις συνδέσεις που ξεκινούν από τον υπολογιστή μας προς ξένους . Είναι , λοιπόν ένα είδος «software firewall» και μπορεί να μας προστατεύσει τόσο από κινδύνους που προέρχονται από το εξωτερικό όσο και από κινδύνους που προέρχονται από το εσωτερικό.

Εδώ θα ήταν καλό να αναφερθεί ότι οποιαδήποτε αλλαγή ρυθμίσεων σε οποιοδήποτε από τα προγράμματα ασφαλείας που μας παρέχονται , θα πρέπει να γίνεται με πάρα πολύ προσοχή. Τις περισσότερες φορές λόγο απροσεξίας μας είτε λόγο άγνοιάς μας , αποδυναμώνουμε από μόνοι μας το σύστημα ασφαλείας μας .

5.1.2.1 Περιγραφή του Windows Firewall

Κεντρικό παράθυρο του Windows Firewall.



Εικόνα 9 : Κεντρικό παράθυρο του Windows Firewall

Στο Αριστερό Μενού παρατηρούμε δύο επιλογές :

1. Ενεργοποίηση ή απενεργοποίηση του τείχους προστασίας των Windows :

Πατώντας την επιλογή αυτή εμφανίζεται το παράθυρο των ρυθμίσεων του Firewall στο οποίο μπορούμε να ρυθμίσουμε αναλυτικά τις λειτουργίες του Firewall μας .

2. Να επιτρέπεται ένα πρόγραμμα μέσω του τείχους προστασίας των Windows

Πατώντας την επιλογή αυτή εμφανίζεται το παράθυρο των εξαιρέσεων του Firewall στο οποίο μπορούμε να ρυθμίσουμε αναλυτικά σε ποια προγράμματα θα επιτρέπεται να εκτελούνται και σε ποια θα απαγορεύεται η δικτυακή σύνδεση με απομακρυσμένες περιοχές .

Παράθυρο ρυθμίσεων του Firewall

Το Παράθυρο των ρυθμίσεων αποτελείται από τρεις καρτέλες .

Την καρτέλα **¨Γενικά¨** , την καρτέλα **¨ Εξαιρέσεις¨** και τέλος την καρτέλα **¨ Για προχωρημένους¨**

Εικόνα 10: Παράθυρο ρυθμίσεων του Windows Firewall.

Στην καρτέλα Γενικά :

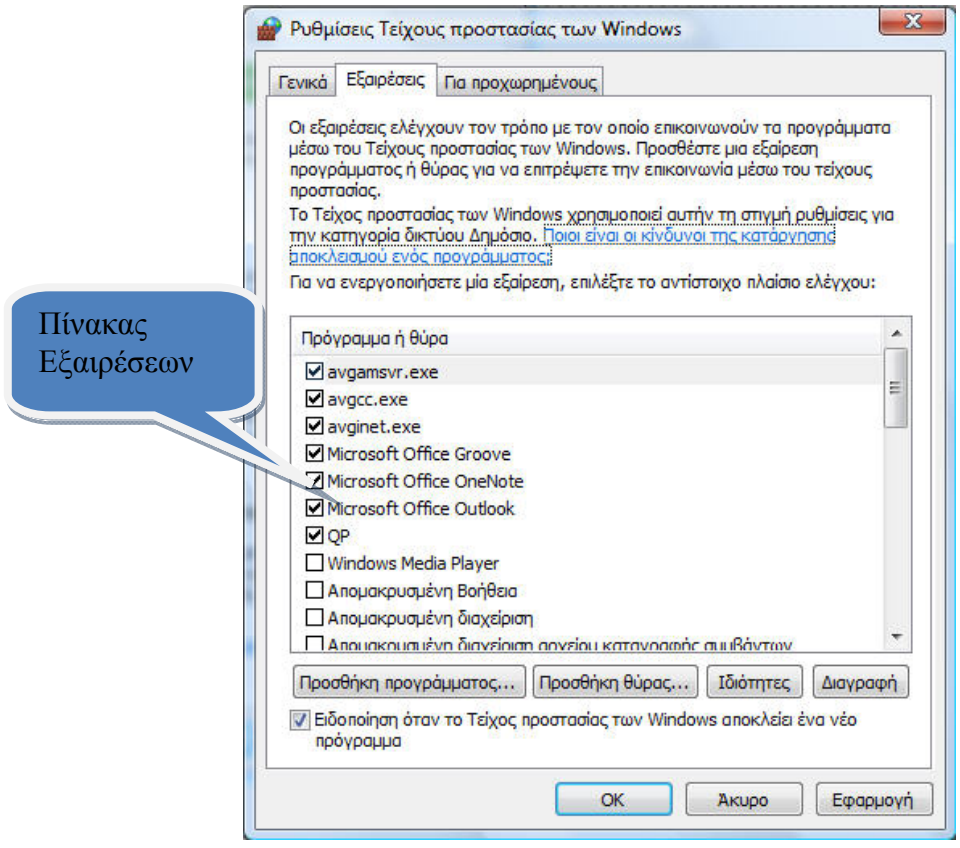
Εμφανίζονται τρείς επιλογές

- Ενεργοποίηση (προτείνεται): Εάν είναι επιλεγμένη αυτή η επιλογή , τότε έχουμε θέσει σε λειτουργία το Τείχος προστασίας μας .
- Απενεργοποίηση(δεν προτείνεται): Εάν είναι επιλεγμένη αυτή η επιλογή ,τότε το Τείχος προστασίας μας είναι ανενεργό.
- Αποκλεισμός όλων των εισερχόμενων συνδέσεων : Εάν είναι επιλεγμένη αυτή η επιλογή ,τότε το Τείχος προστασίας μας αποκλείει όλες τις αυτόκλητες προσπάθειες για σύνδεση με τον υπολογιστή μας . Η επιλογή αυτή προτείνεται όταν επιθυμούμαι μέγιστη ασφάλεια , καθώς και όταν είμαστε συχνοί χρήστες δημόσιων δικτύων που οι κίνδυνοι από κακόβουλα λογισμικά αυξάνονται . Τέλος με αυτήν την ρύθμιση δεν θα λαμβάνουμε ειδοποίηση όταν το τείχος προστασίας μας θα αποκλείει ένα πρόγραμμα και θα γίνεται παράβλεψη των προγραμμάτων που βρίσκονται στην λίστα ¨Εξαιρέσεις¨

Στην καρτέλα Εξαιρέσεις :

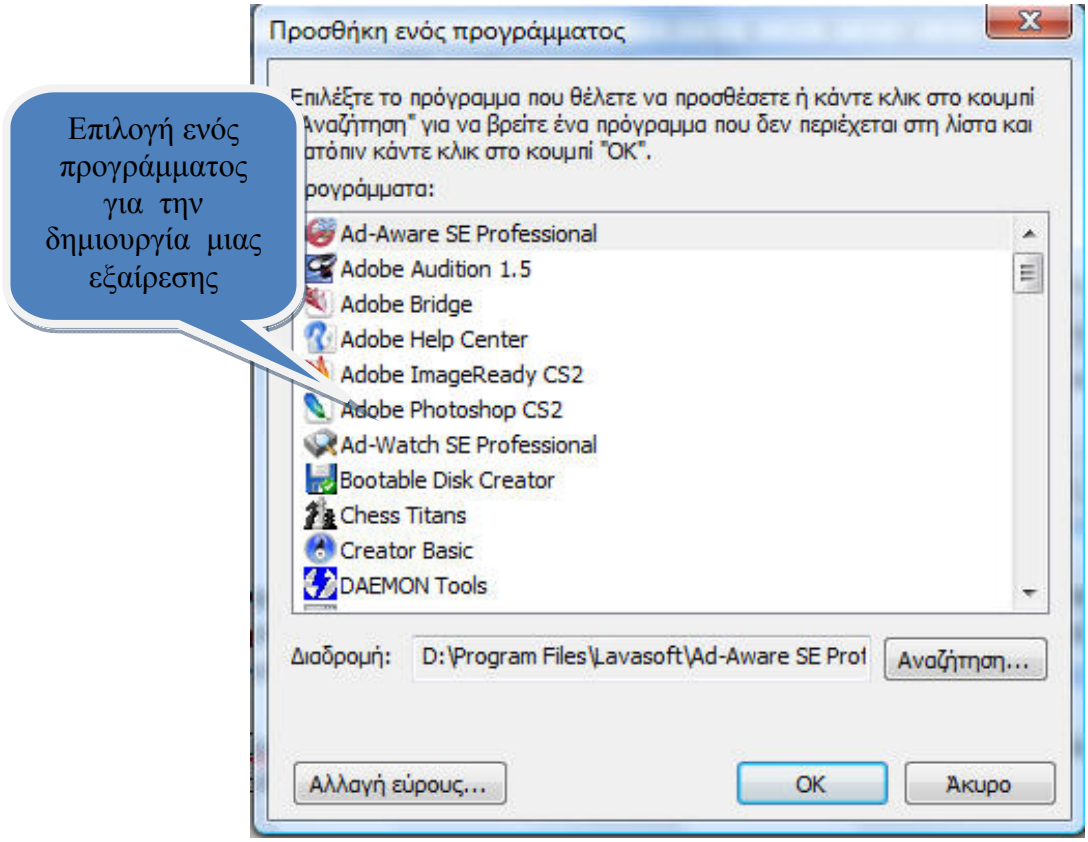
Γίνεται έλεγχος του τρόπου με τον οποίο επικοινωνούν τα προγράμματα μέσω του Τείχους προστασίας . Έχουμε την δυνατότητα εδώ να ενεργοποιήσουμε ή να απενεργοποιήσουμε κάποια εξαίρεση (δηλαδή κάποιο πρόγραμμα στο οποίο επιτρέπουμε ή όχι ελεύθερη πρόσβαση.)

Παρατηρούμε έναν πίνακα με προγράμματα , τα προγράμματα αυτά μπορούμε είτε να τα διαλέξουμε, κάνοντάς τα έτσι ¨εξαίρεση¨ , είτε να μην τα διαλέξουμε.



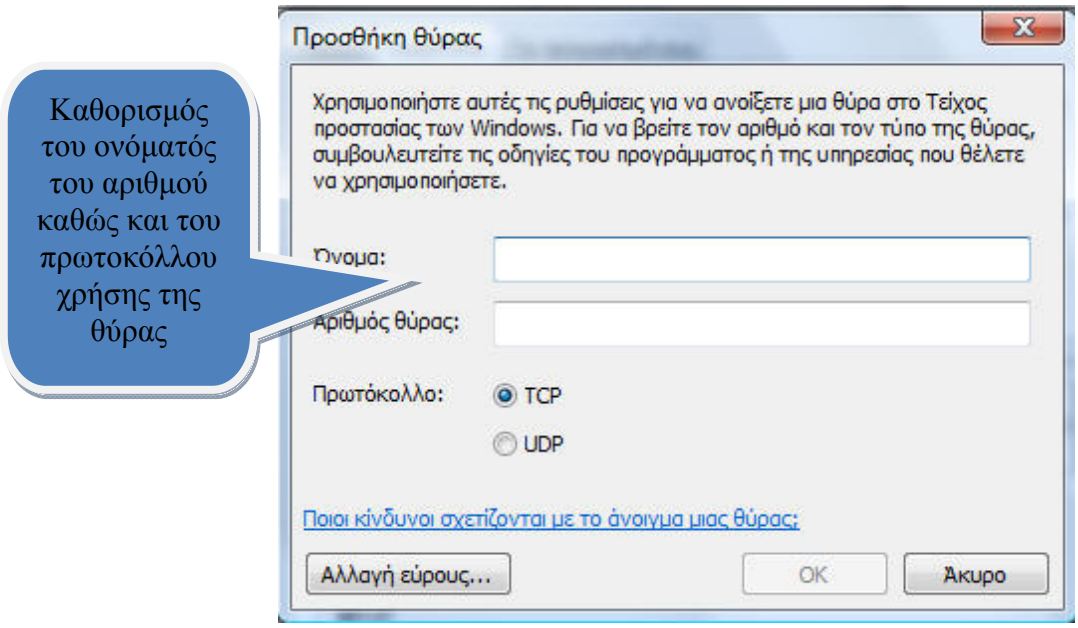
Εικόνα 11:Πίνακας εξαιρέσεων του Windows Firewall .

Έχουμε την δυνατότητα επίσης να δημιουργήσουμε εμείς προσωπικές εξαιρέσεις . Εάν κάποιο πρόγραμμα το οποίο δεν εμφανίζεται στον πίνακα και το οποίο εμείς θέλουμε να κάνουμε εξαίρεση, μπορούμε να το προσθέσουμε από την επιλογή **Προσθήκη προγράμματος .**



Εικόνα 12: Παράθυρο δημιουργίας εξαίρεσης από τον χρήστη.

Ομοίως μπορούμε να ανοίξουμε κάποια θύρα στο Τείχος προστασίας . Πατώντας στην επιλογή Προσθήκης θύρας και ρυθμίζοντας κάποιες επιλογές .



Εικόνα 13: Παράθυρο προσθήκης θύρας TCP/UTP στις εξαιρέσεις του Windows Firewall.

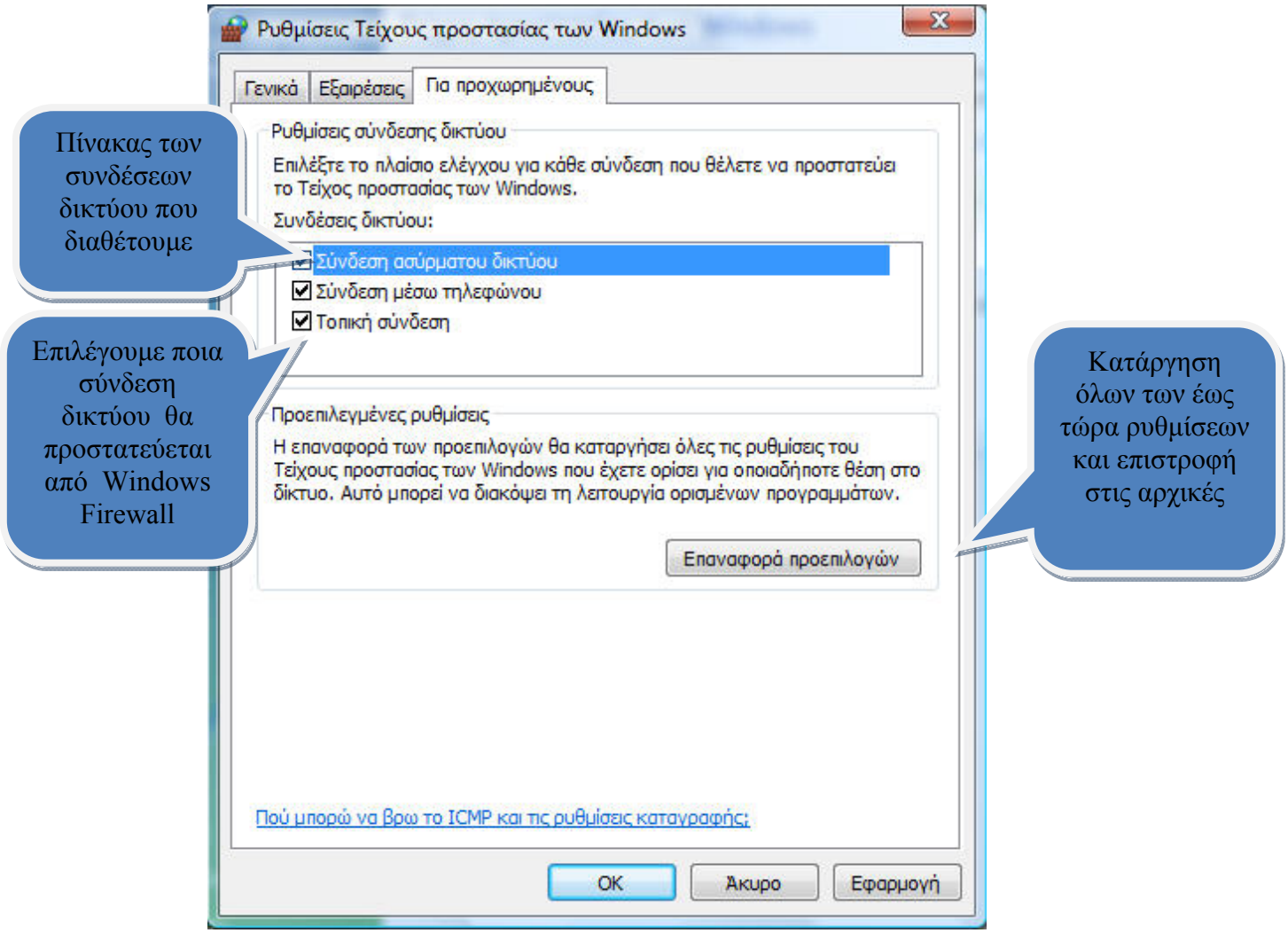
Πατώντας στην επιλογή **Ιδιότητες** στην καρτέλα **Εξαιρέσεις** μπορούμε να επεξεργαστούμε ξεχωριστά κάποιο από τα προγράμματα του πίνακα των εξαιρέσεων και να το ρυθμίσουμε όσον αφορά το Τείχος προστασίας.

Τέλος με την επιλογή **Διαγραφή** μπορούμε να διαγράψουμε κάποια από τις εξαιρέσεις μας .

Στην καρτέλα Για προχωρημένους :

Εμφανίζεται ένας πίνακας των συνδέσεων μέσω των οποίων είχαμε ή μπορούμε να έχουμε πρόσβαση στο δίκτυο . Έχουμε την δυνατότητα να επιλέξουμε την σύνδεση την όποια επιθυμούμε να προστατεύει το Τείχος προστασίας.

Στην καρτέλα αυτή υπάρχει και η επιλογή **Επαναφορά προεπιλογών**. Πατώντας στην επιλογή αυτή όλες οι ρυθμίσεις τις οποίες έχουμε κάνει και αφορούν το Τείχος προστασίας θα χαθούν και θα γίνει επαναφορά των εργοστασιακών ρυθμίσεων .



Εικόνα 14: Καρτέλα για προχωρημένους χρήστες του Windows Firewall.

Στο δεξί μενού του Τείχους προστασίας μας δίνεται η δυνατότητα να επέμβουμε στις ρυθμίσεις του τείχους .

Πατώντας στο **Αλλαγή Ρυθμίσεων** εμφανίζεται πάλι το παράθυρο Ρυθμίσεις Τείχους προστασίας των Windows , το οποίο και αναλύσαμε προηγουμένως .

Οι επιλογές που μας εμφανίζονται στο παράθυρο αυτό είναι οι ακόλουθες :

- Ενεργοποίηση
- Απενεργοποίηση.
- Αποκλεισμός όλων των εισερχόμενων συνδέσεων .

Τις δύο πρώτες επιλογές τις έχουμε είδη επεξηγήσει ,η τρίτη επιλογή αυτή δηλαδή του αποκλεισμού όλων των εισερχόμενων συνδέσεων έχει να κάνει με το εάν επιτρέπουμε ή όχι να συνδεθεί ο υπολογιστής μας με οποιαδήποτε εξωτερική σύνδεση .’

Η επιλογή αυτή είναι πολύ χρήσιμη ιδιαίτερα σε δημόσια δίκτυα υπολογιστών.

5.1.2.2 Εκδόσεις του Windows Firewall

- **Windows XP:** Το Windows Firewall πρωτοπαρουσιάστηκε ως κομμάτι του Service Pack 2 των Windows XP. Κάθε τύπος δικτυακής σύνδεσης , είτε ήταν ενσύρματης , ασύρματης , VPN ακόμη και FireWire έχει το firewall ενεργό εξ ορισμού με κάποιες επιπλέον ενσωματωμένες εξαιρέσεις προκειμένου να επιτρέπεται η σύνδεση μηχανημάτων τα οποία βρίσκονται στο τοπικό δίκτυο .
  Περιλαμβάνει επίσης και τον νέο όρο **Group policy** , πολιτικές μέσω των οποίων οι διαχειριστές των συστημάτων μπορούσαν να ρυθμίσουν το Windows Firewall ανάλογα ο καθένας με τις προσωπικές του απαιτήσεις είτε τις απαιτήσεις των μελών του εκάστοτε γκρουπ. Το Firewall Windows XP δεν έχει την δυνατότητα να μπλοκάρει τις εξερχόμενες συνδέσεις είναι σε θέση μόνο να μπλοκάρει τις εισερχόμενες .

- **Windows Server 2003:** Τον Μάιο του 2005, η Microsoft κυκλοφόρησε το Windows Server 2003 Service Pack 1, στο οποίο ενσωμάτωσε τις ίδιες βελτιώσεις τις οποίες ενσωμάτωσε και στο λειτουργικό σύστημα του server.

- **Windows Vista:** Τα Windows Vista βελτίωσαν σημαντικά το firewall ειδικά σε θέματα που απασχολούσαν την λειτουργικότητα του firewall σε εταιρικό περιβάλλον.

  - Με μια νέα **διαχειριστική κονσόλα** είναι εφοδιασμένο το νέο firewall με την ονομασία **Windows Firewall with Advanced Security** . Η κονσόλα αυτή παρέχει πρόσβαση σε πολλές προχωρημένες ρυθμίσεις καθώς επίσης καθιστά ενεργή την απομακρυσμένη διαχείριση . Η πρόσβαση αυτή πετυχαίνεται ακολουθώντας τα παρακάτω βήματα **Έναρξη ->Πίνακας Ελέγχου -> Διαχειριστικά Εργαλεία -> Τείχος προστασίας των Windows με εξελιγμένη ασφάλεια ..** ή πατώντας την εντολή **wf.msc** στο πλαίσιο της αναζήτησης .
  - **IPv6** φιλτράρισμα συνδέσεων.
  - **Φιλτράρισμα εξερχόμενων πακέτων** , αυξάνοντας θετικά την προστασία κατά των spyware και των virus . **Εξερχόμενες ρυθμίσεις** και **κανόνες** χρησιμοποιούνται από την κονσόλα διαχείρισης .
  - Με το **προχωρημένο πακέτο φιλτραρίσματος** , οι κανόνες μπορούν να προσαρμόζονται και να εφαρμόζονται σε συγκεκριμένους πόρους , προορισμούς ip διευθύνσεων και σε συγκεκριμένο εύρος πυλών .
  - Το **IPSec** είναι πλήρως ενσωματωμένο ,και παρέχει την δυνατότητα στις συνδέσεις να επιτρέπονται ή να απορρίπτονται βάση κάποιων πιστοποιητικών ασφάλειας .Κρυπτογράφηση μπορεί ακόμη να ζητηθεί για οποιοδήποτε είδος σύνδεσης .
  - Ικανότητα να διαθέτει διαφορετικά προφίλ firewall για τους υπολογιστές που συνδέονται είτε σε κάποιον τομέα είτε συνδέονται σε ένα ιδιωτικό ή δημόσιο δίκτυο . Τέλος υποστηρίζει την δημιουργία κανόνων και πολιτικών απομόνωσης κεντρικών υπολογιστών και περιοχών .

- **Windows Server 2008:** Αυτή η έκδοση του λογισμικού περιέχει το ίδιο firewall με τα Windows Vista.

5.1.2.3 Πως λειτουργεί το Firewall των Windows Vista .

Το Windows Firewall , είναι ένα προσωπικό Firewall ,το οποίο περιλαμβάνεται στα τελευταία λειτουργικά συστήματα της Microsoft , Windows XP ,Vista .

Όταν τα Windows XP άρχισαν να πρωτοεμφανίζονται τον Οκτώβριο του 2001 , περιλάμβαναν ένα περιορισμένο firewall το οποίο ονομαζόταν **¨Internet Connection Firewall¨** . Το firewall αυτό ήταν ανενεργό εξ ορισμού λόγω των περιορισμένων δυνατοτήτων του ,παρόλα αυτά διέθετε πολλές προς τα πίσω συμβατότητες . Στα μέσα του 2003 εμφανίστηκαν οι επιθέσεις των **Blaster worms** , ένα μεγάλο μέρος των μηχανημάτων της εποχής εκείνης εκτέθηκαν από αυτού του είδους τις επιθέσεις , οι οποίες εκμεταλλευόντουσαν τις ρωγμές που εμφάνιζαν οι RPC Windows Service . Μερικούς μήνες αργότερα εμφανίστηκαν και **Sasser worms** τα οποία έκαναν παρόμοια δουλειά με τα προαναφερθέντα.

Λόγω αυτών των γεγονότων καθώς επίσης λόγω της ελλιπούς προστασίας που παρείχε το firewall, η Microsoft αποφάσισε να βελτιώσει τόσο την λειτουργία όσο και την διεπαφή της ενσωματωμένης αντιπυρικής ζώνης των Windows XP και δημιούργησε έτσι το καινούργιο firewall γνωστό ως ¨Windows Firewall¨.

Ο τρόπος λειτουργίας ενός Firewall είναι απλός. Έστω ότι κάποιος χρήστης του Internet ή κάποιος στο δίκτυο προσπαθεί να συνδεθεί στον υπολογιστή μας , καλούμε αυτήν την προσπάθεια **¨εκούσια προσπάθεια (unsolicited request) ¨** . Όταν τώρα υπολογιστής μας δεχτεί μια τέτοια εκούσια προσπάθεια , το Windows Firewall μπλοκάρει την σύνδεση αυτή και ταυτόχρονα μας ειδοποιεί για την ενέργεια του αυτή.

Εικόνα 15 : Παράθυρο ειδοποίησης του Windows Firewall.

Εάν τρέχουμε κάποιο πρόγραμμα άμεσης αποστολής μηνυμάτων όπως πχ το windows live messenger ή αν παίζουμε κάποιο δικτυακό παιχνίδι το οποίο χρειάζεται να λαμβάνει πληροφορίες από το Internet ή από το δίκτυο , το Firewall μας ειδοποιεί και μας ρωτάει εάν θέλουμε να επιτρέψουμε ή να απαγορέψουμε την σύνδεση αυτή.

Στην περίπτωση που επιλέξουμε να επιτραπεί η σύνδεση το firewall δημιουργεί μια εξαίρεση για το συγκεκριμένο πρόγραμμα έτσι ώστε να μην μας ενοχλεί με ειδοποιήσεις κάθε φορά που επιθυμούμε να ξαναχρησιμοποιήσουμε το πρόγραμμα αυτό.

5.1.2.4 Ρύθμιση του Windows Firewall στα Vista

Με το να ρυθμίζουμε το Windows Firewall , δημιουργούμε κανόνες τείχους προστασίας για να επιτρέψουμε στον υπολογιστή μας να αποστέλλει δεδομένα προς ή να λαμβάνει δεδομένα από προγράμματα , υπηρεσίες συστήματος υπολογιστές ή χρήστες .

Μπορούμε να δημιουργήσουμε κανόνες τείχους προστασίας οι οποίοι θα πραγματοποιούν μια από τις τρείς διαθέσιμες ενέργειες για όλες τις συνδέσεις που πληρούν τα κριτήρια του κανόνα : να επιτρέπουν την σύνδεση , να επιτρέπουν μόνο μια σύνδεση που προστατεύεται από την ασφάλεια πρωτοκόλλου Internet (IPsec), ή να αποκλείουν ρητά την σύνδεση .

Οι κανόνες αυτοί που δημιουργούμε μπορούν να ρυθμιστούν είτε για την εισερχόμενη είτε για την εξερχόμενη κυκλοφορία . Ο κάθε κανόνας μπορεί να ρυθμιστεί έτσι ώστε να καθορίζει τους υπολογιστές ή τους χρήστες , το πρόγραμμα , την υπηρεσία ή την θύρα και το πρωτόκολλο .
Μπορούμε να καθορίσουμε τον τύπο του προσαρμογέα δικτύου , στον οποίο θα εφαρμόζεται ο κανόνας : Τοπικό δίκτυο (LAN) , ασύρματο , απομακρυσμένη πρόσβαση ,για παράδειγμα μια σύνδεση εικονικού ιδιωτικού δικτύου (VPN), ή όλους τους τύπους . Μπορούμε ακόμη να ρυθμίσουμε τις παραμέτρους του εφαρμοζόμενου κανόνα , όταν χρησιμοποιούμε ένα συγκεκριμένο προφίλ ή όταν χρησιμοποιούμε ένα οποιοδήποτε προφίλ.

Καθώς το περιβάλλον τεχνολογιών πληροφορικής μεταβάλλεται , είναι πιθανόν να χρειαστεί να αλλάξουμε , να δημιουργήσουμε , να απενεργοποιήσουμε ή να διαγράψουμε κανόνες .

Οι κανόνες τείχους προστασίας εφαρμόζονται με την ακόλουθη σειρά προτεραιότητας :

- Παράκαμψη ελέγχου ταυτότητας (με άλλα λόγια , κανόνες που παρακάμπτουν κανόνες αποκλεισμού).
- Αποκλεισμός σύνδεσης .
- Να επιτρέπεται η σύνδεση .
- Συμπεριφορά προεπιλεγμένου προφίλ (να επιτρέπεται ή να αποκλείεται η σύνδεση σύμφωνα με την καρτέλα **Προφίλ** του παραθύρου διαλόγου **Ιδιότητες Τείχους προστασίας των Windows με Ασφάλεια για προχωρημένους**).

Κανόνες εισερχόμενων : Οι κανόνες εισερχόμενων επιτρέπουν ή απαγορεύουν ρητώς την κυκλοφορία που πληροί τα κριτήρια του κανόνα . Για παράδειγμα μπορούμε να ρυθμίσουμε τις παραμέτρους ενός κανόνα , ώστε να επιτρέπει ρητώς την διέλευση από το τείχος προστασίας της

κυκλοφορίας , η οποία προστατεύεται από την IPsec απομακρυσμένης επιφάνειας εργασίας , αλλά να αποκλείει την ίδια την κυκλοφορία , εάν δεν προστατεύεται από την IPsec. Όταν εγκαθιστούνται τα Windows για πρώτη φορά , αποκλείεται η κυκλοφορία εισερχομένων. Για να επιτραπεί η κυκλοφορία θα πρέπει να δημιουργήσουμε έναν κανόνα εισερχομένων. Επίσης μπορούμε να ρυθμίσουμε τις παραμέτρους της ενέργειας που κάνει το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους , αν επιτρέπονται ή αποκλείονται οι συνδέσεις , πότε θα εφαρμόζεται καθένας κανόνας .

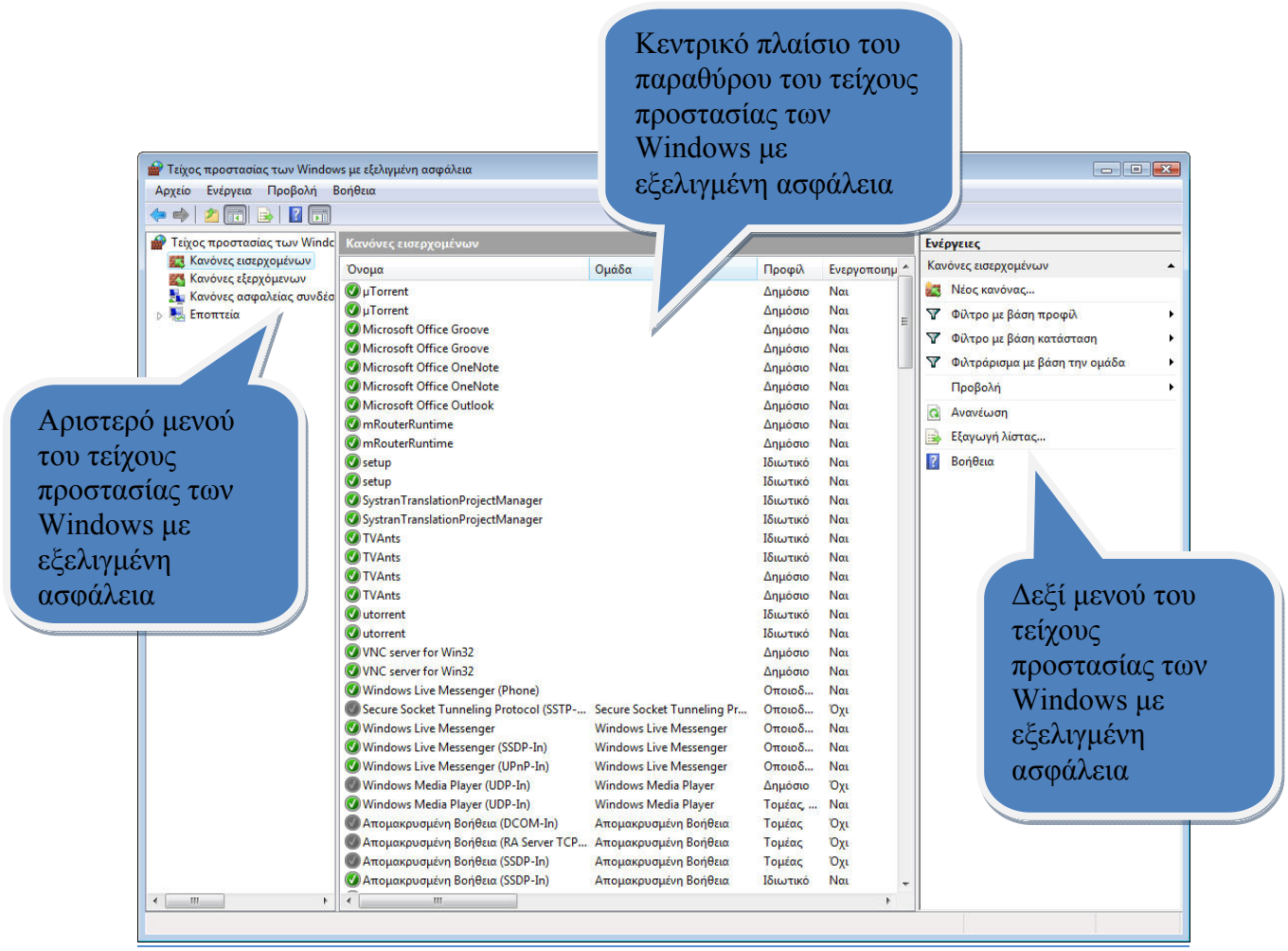
Κανόνες εξερχομένων : Οι κανόνες εξερχομένων επιτρέπουν ή απαγορεύουν ρητώς την κυκλοφορία που προέρχεται από τον υπολογιστή , ο οποίος πληροί τα κριτήρια του κανόνα . Για παράδειγμα μπορούμε να ρυθμίσουμε τις παραμέτρους ενός κανόνα , ώστε να αποκλείει ρητώς την εξερχόμενη κυκλοφορία προς κάποιον υπολογιστή μέσω του τείχους προστασίας , ενώ θα επιτρέπει την ίδια την κυκλοφορία προς άλλους υπολογιστές . Η εξερχόμενη κυκλοφορία επιτρέπεται από προεπιλογή . Συνεπώς για να αποκλείσουμε την κυκλοφορία αυτή θα πρέπει να δημιουργήσουμε έναν κανόνα εξερχομένων.

Η προεπιλεγμένη ενέργεια , δηλαδή το εάν θα επιτρέπονται ή θα αποκλείονται οι συνδέσεις από προεπιλογή , μπορεί να ρυθμιστεί .

Η ρύθμιση του Windows Firewall επιτυγχάνεται μέσα από τα διαχειριστικά εργαλεία και συγκεκριμένα από το παράθυρο του τείχους προστασίας των Windows με εξελιγμένη ασφάλεια .

Όπως προαναφέραμε για να εμφανίσουμε το παράθυρο αυτό ακλουθούμε το μονοπάτι είτε μέσω του πίνακα ελέγχου και των διαχειριστικών εργαλείων είτε μέσω της εντολής wf.msc στο πλαίσιο της αναζήτησης.

Παράθυρο του τείχους προστασίας των Windows με εξελιγμένη ασφάλεια.



Εικόνα 16 : Παράθυρο τείχος προστασίας των Windows με εξελιγμένη ασφάλεια .

Μέσω αυτού του παραθύρου μπορούμε να παρακολουθήσουμε να δημιουργήσουμε ή να καταργήσουμε κανόνες με βάση τους οποίους λειτουργεί το τείχος προστασίας μας .
Όπως έχουμε ήδη εξηγήσει το νέο και βελτιωμένο αυτό τείχος προστασίας μπορεί να ρυθμίσει κανόνες τόσο για την εισερχόμενη κίνηση όσο και για την εξερχόμενη .

Στο Αριστερό μενού βρίσκονται οι επιλογές :

- **Κανόνες εισερχόμενων :** Πατώντας αυτήν την επιλογή στο κεντρικό πλαίσιο του παραθύρου εμφανίζονται όλες εκείνες οι υπηρεσίες και τα προγράμματα στα οποία έχει εφαρμοστεί κάποιος κανόνας εισερχόμενης κυκλοφορίας , καθώς και άλλες λεπτομέρειες σχετικές με αυτά , όπως το προφίλ τους , την ενέργεια που εκτελείται σε αυτά κ.α.
- **Κανόνες εξερχόμενων :** Πατώντας την δεύτερη αυτή επιλογή , στο κεντρικό πλαίσιο εμφανίζονται όλες εκείνες οι υπηρεσίες και τα προγράμματα στα οποία έχει εφαρμοστεί κάποιος κανόνας εξερχομένης κυκλοφορίας , καθώς και άλλες λεπτομέρειες σχετικές με αυτά , όπως το προφίλ τους , την ενέργεια που εκτελείται σε αυτά κ.α.
- **Κανόνες ασφάλειας συνδέσεως :** Πατώντας την επιλογή αυτή , στο κεντρικό παράθυρο εμφανίζονται όλες εκείνες οι υπηρεσίες και τα προγράμματα στα οποία έχει εφαρμοστεί

κάποιος κανόνας ασφάλειας συνδέσεως , καθώς και άλλες λεπτομέρειες σχετικές με αυτά , όπως το προφίλ τους , την ενέργεια που εκτελείται σε αυτά κ.α.

- **Εποπτεία :** Τέλος υπάρχει και η επιλογή εποπτεία , πατώντας την επιλογή αυτή στο κεντρικό παράθυρο εμφανίζονται όλες οι ενέργειες που είναι σε εφαρμογή , καθώς μέσω αυτού του παραθύρου μπορούμε να εποπτεύουμε όλους τους κανόνες και ενέργειες που σχετίζονται με το τείχος προστασίας .

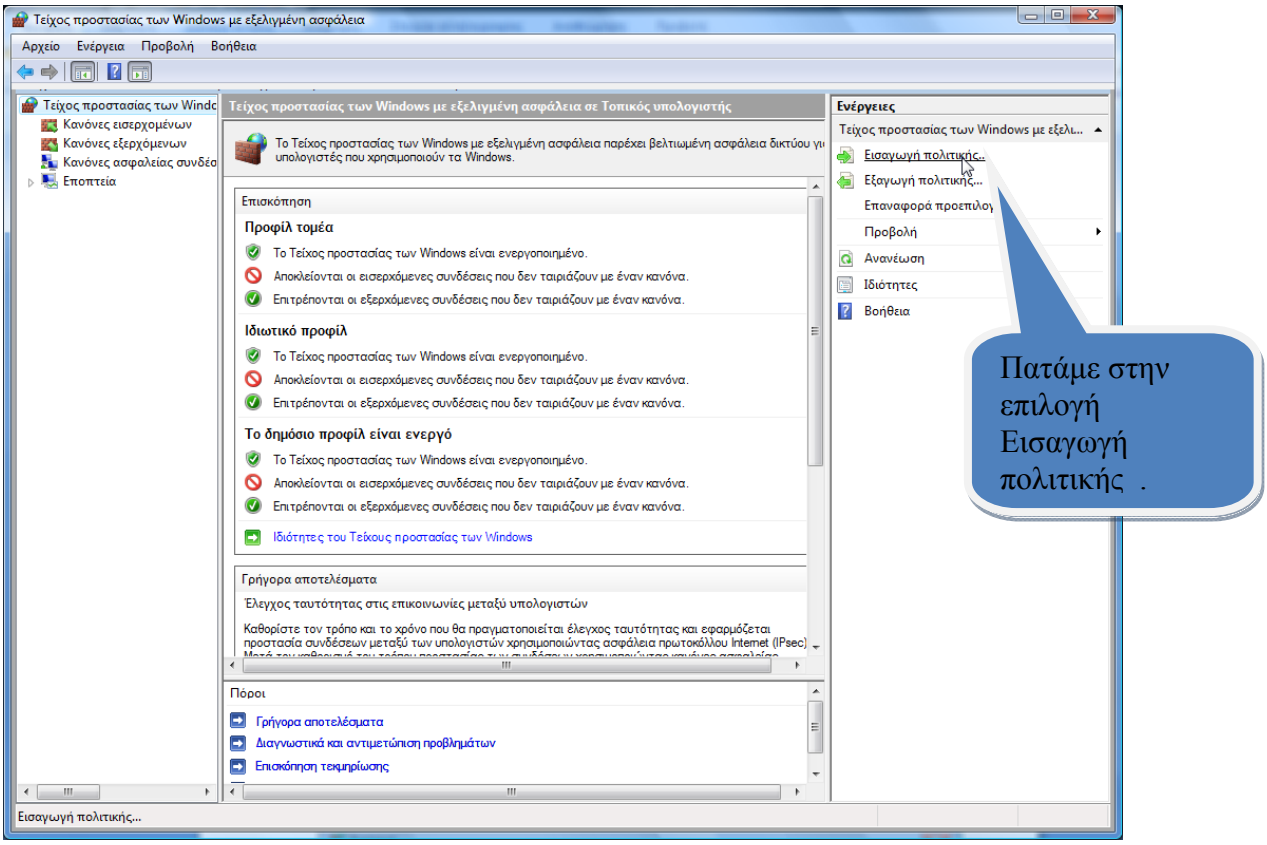
Στο Δεξί μενού βρίσκονται οι επιλογές :

Εισαγωγή πολιτικής , εξαγωγή πολιτικής , επαναφορά προεπιλογών , προβολή , ανανέωση , ιδιότητες κ.α.
Όλες οι επιλογές σχετίζονται με τις πολιτικές και γενικά με ότι σχετίζονται με αυτές , δηλαδή το πώς δημιουργούνται , αφαιρούνται και γενικά το πώς ρυθμίζονται .

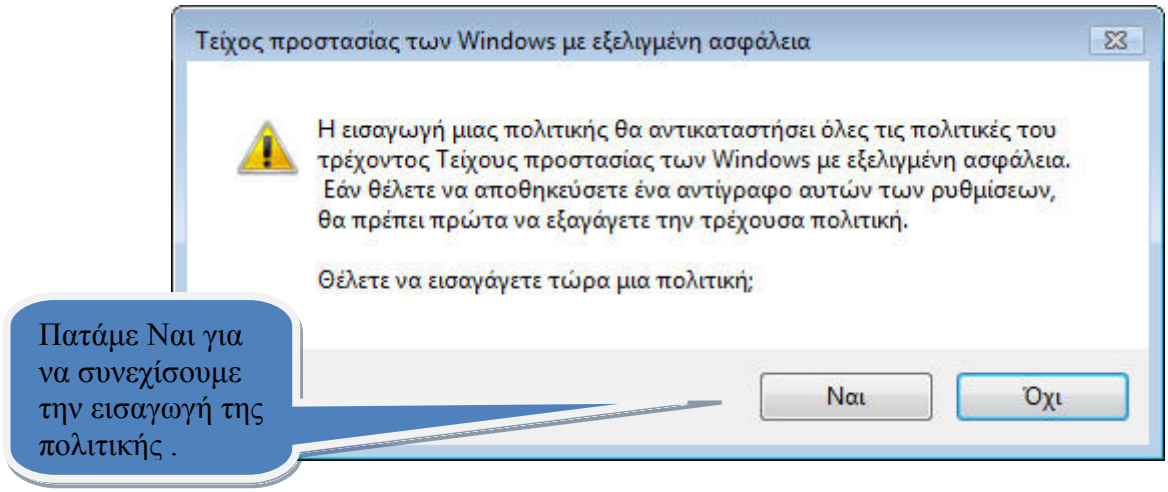
Στο σημείο αυτό θα περιγράψουμε πως μπορούμε να κάνουμε εισαγωγή μιας πολιτικής , εξαγωγή μιας πολιτικής και τέλος να δημιουργήσουμε έναν νέο κανόνα .

Εισαγωγή μιας πολιτικής

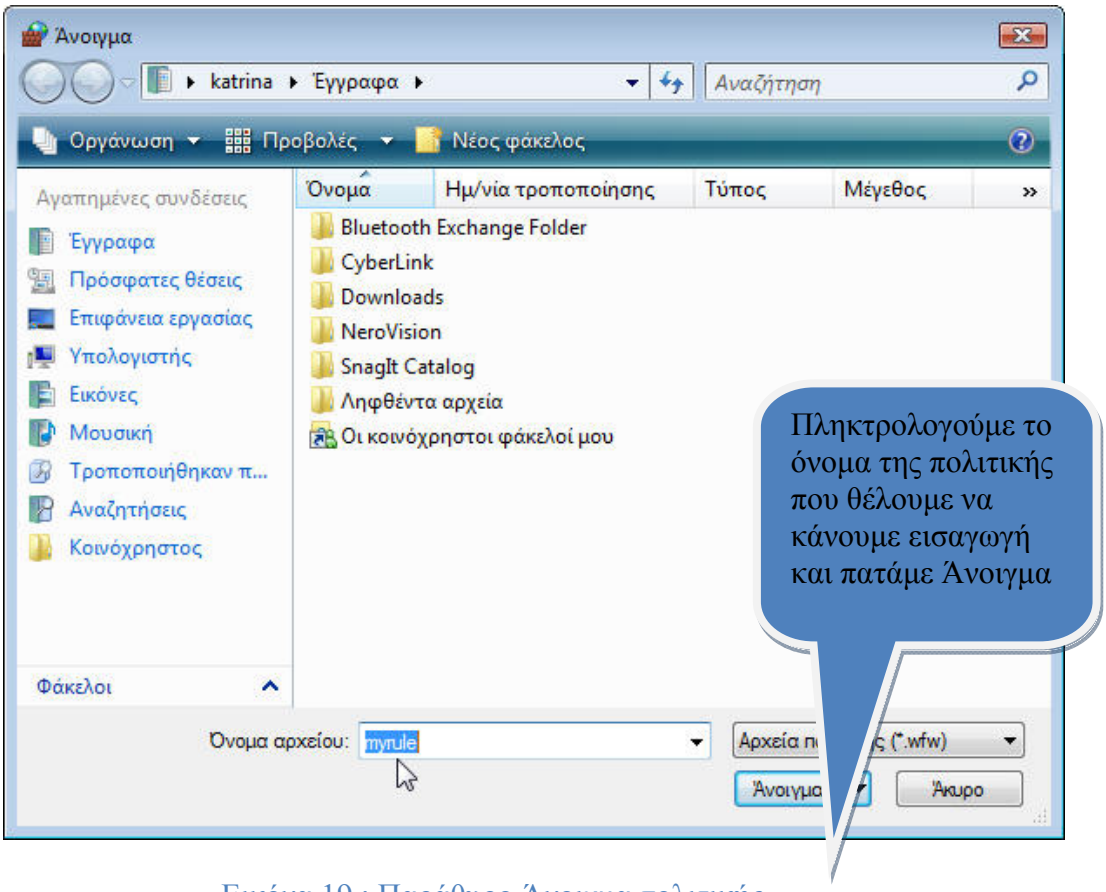
Για να κάνουμε εισαγωγή μιας πολιτικής, δηλαδή για να ανοίξουμε και να εφαρμόσουμε μια πολιτική , πατάμε στην αντίστοιχη επιλογή στο δεξί μενού του παράθυρου Τείχος προστασίας των Windows με εξελιγμένη ασφάλεια .
Στην συνέχεια πατάμε **Ναι** στο παράθυρο ειδοποίησης που εμφανίζεται και έπειτα πατάμε το όνομα τις πολιτικής αυτής στο πλαίσιο όνομα αρχείου και πατάμε **Άνοιγμα .**



Εικόνα 17 : Παράθυρο τείχος προστασίας των Windows με εξελιγμένη ασφάλεια .



Εικόνα 18 : Παράθυρο προειδοποίησης του τείχους προστασίας των Windows με εξελιγμένη ασφάλεια .

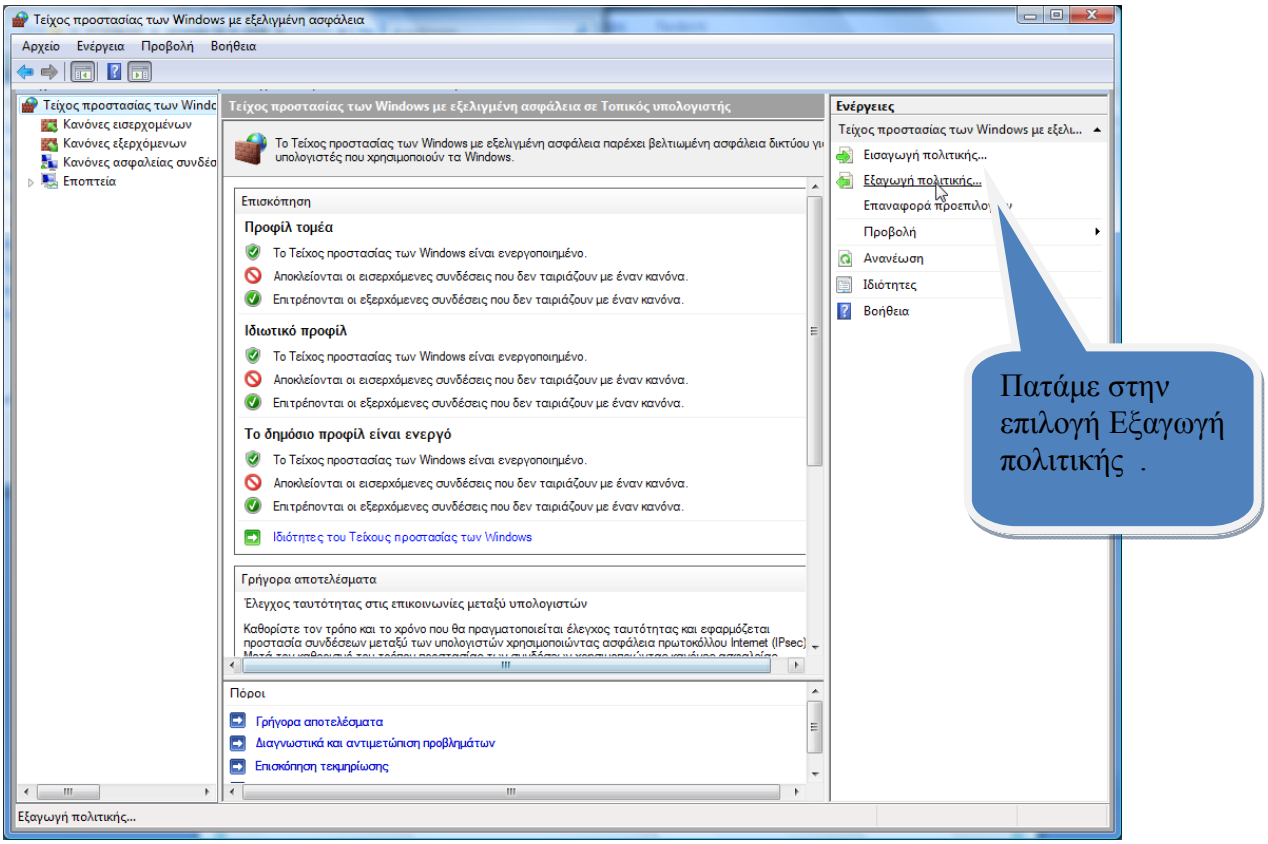


Εικόνα 19 : Παράθυρο Άνοιγμα πολιτικής.

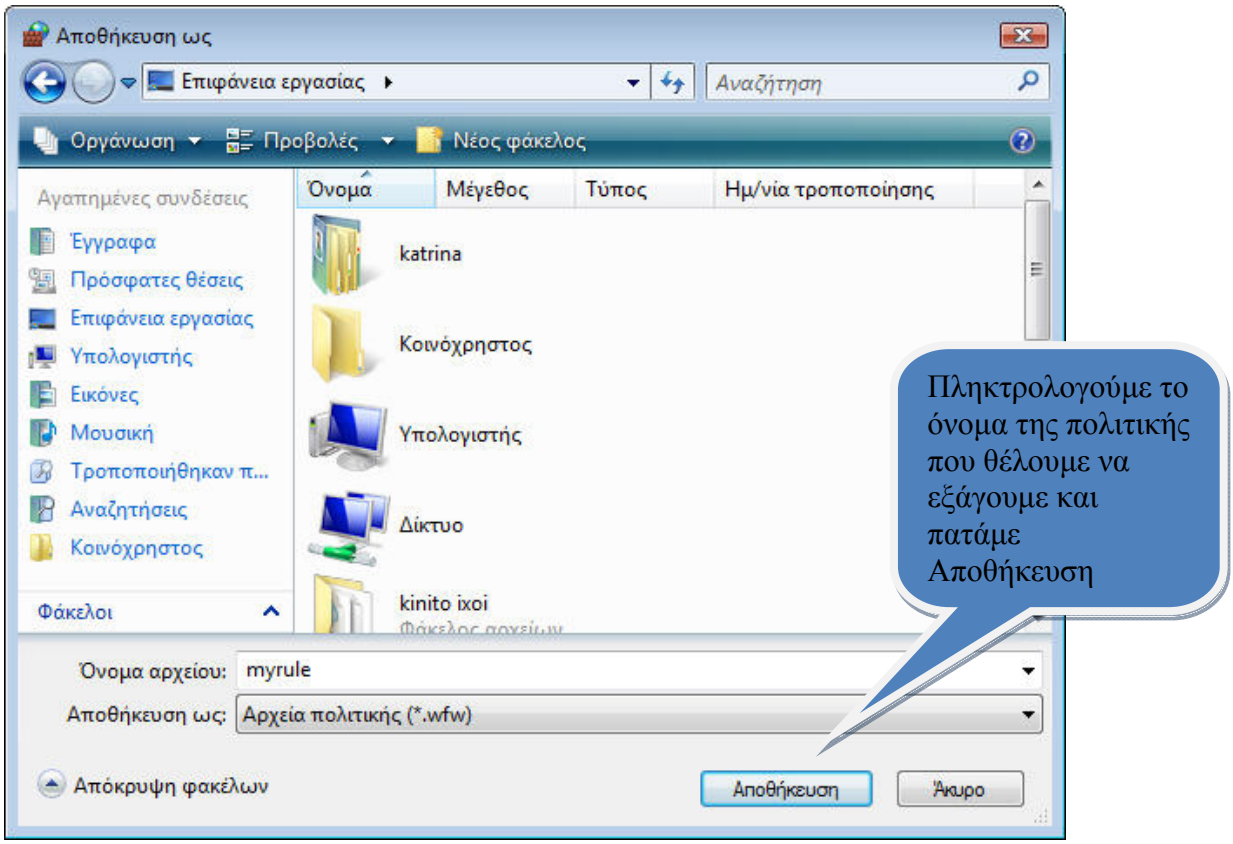
Εξαγωγή μιας πολιτικής

Με παρόμοια βήματα μπορούμε να πραγματοποιήσουμε και την διαδικασία της εξαγωγής μιας πολιτικής .

Αρχικά πατάμε στην επιλογή **Εξαγωγή μιας πολιτικής** . Στην συνέχεια πληκτρολογούμε το όνομα που θέλουμε να δώσουμε στην πολιτική και πατάμε **Αποθήκευση .**



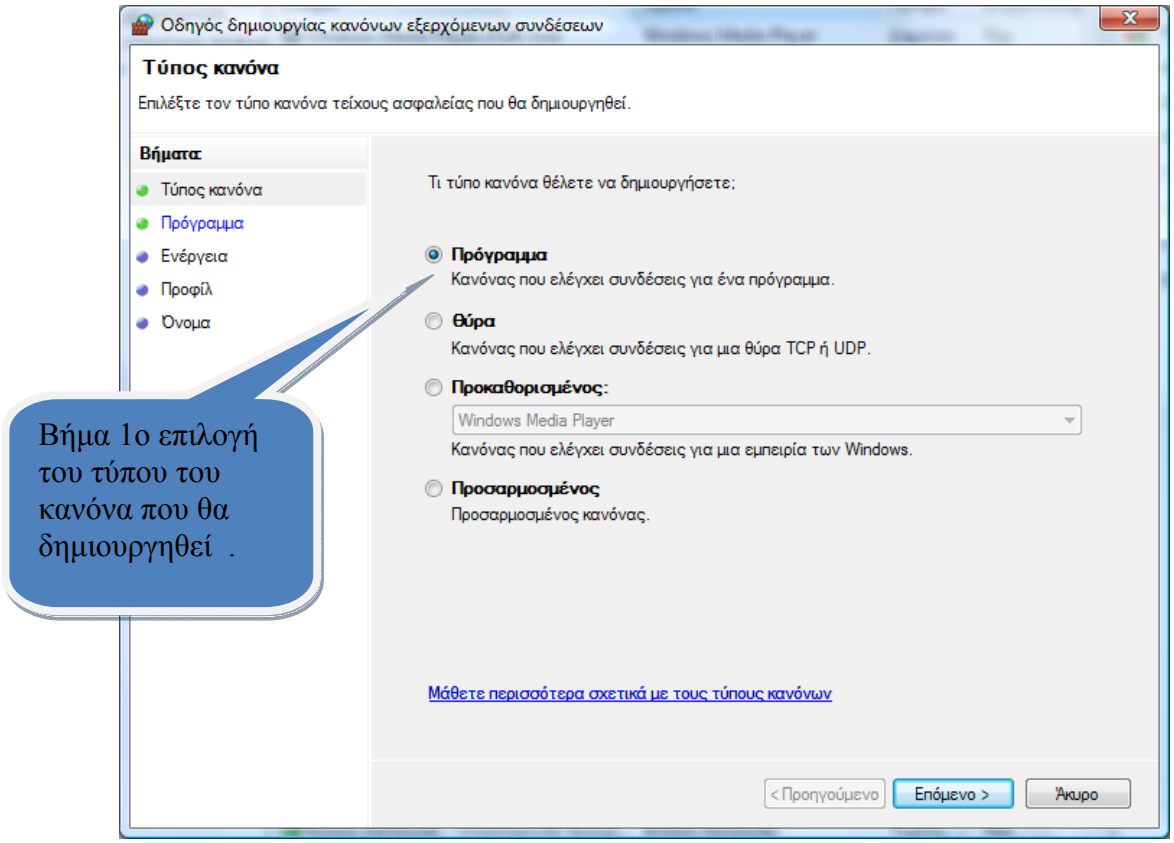
Εικόνα 20 : Παράθυρο τείχος προστασίας των Windows με εξελιγμένη ασφάλεια .



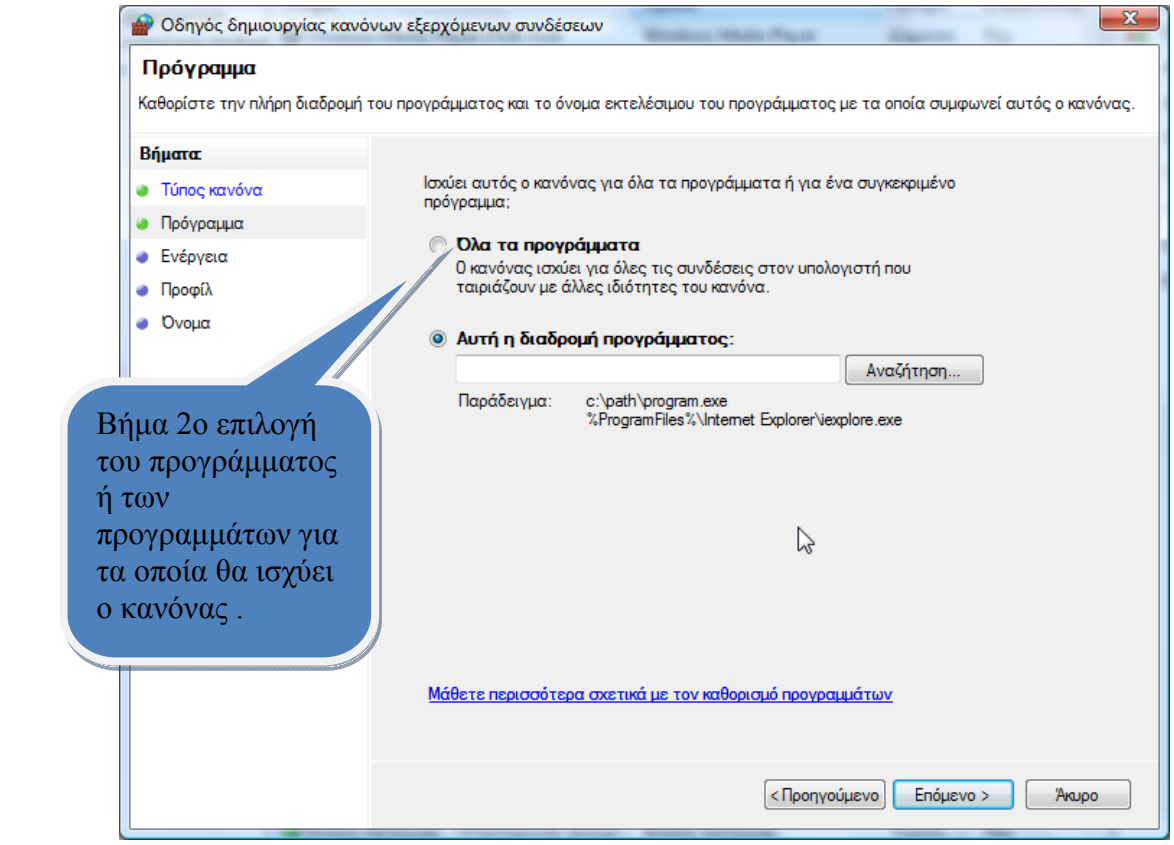
Εικόνα 21: Παράθυρο Αποθήκευση πολιτικής .

Δημιουργία νέου κανόνα

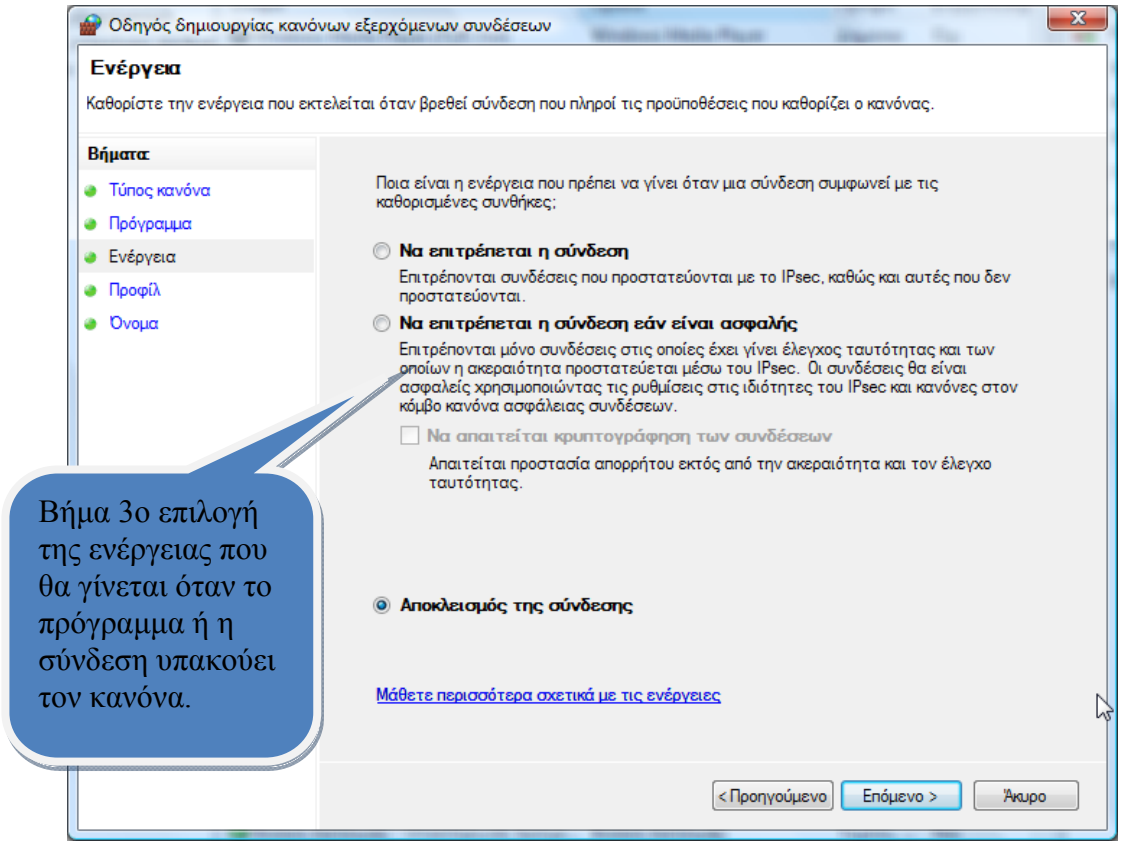
Έχουμε την δυνατότητα να δημιουργήσουμε είτε έναν νέο εισερχόμενο κανόνα είτε έναν νέο εξερχόμενο κανόνα . Τα βήματα που ακολουθούμε είναι ακριβώς τα ίδια . Αρχικά πατάμε στην επιλογή **Νέος κανόνας** στο δεξί μενού του κεντρικού παραθύρου του τείχους προστασίας των Windows με εξελιγμένη ασφάλεια.
Στην συνέχεια επιλέγουμε **τι τύπου θα είναι ο κανόνας** που θα δημιουργήσουμε (Πρόγραμμα , Θύρα , Προκαθορισμένος, Προσαρμοσμένος).
Αφού επιλέξουμε τον τύπο , θα πρέπει να προσδιορίσουμε **σε ποιό πρόγραμμα ή σε ποιά προγράμματα** θα εφαρμοστεί αυτός ο κανόνας .
Ακολουθεί **η επιλογή της ενέργειας** που θα εφαρμοστεί στον κανόνα αυτό . Επόμενο βήμα είναι η **επιλογή του πότε θα ισχύει** ο κανόνας αυτός , και τέλος **επιλέγουμε το όνομα** που θα δώσουμε στον κανόνα αυτόν ολοκληρώνοντας την δημιουργία του .



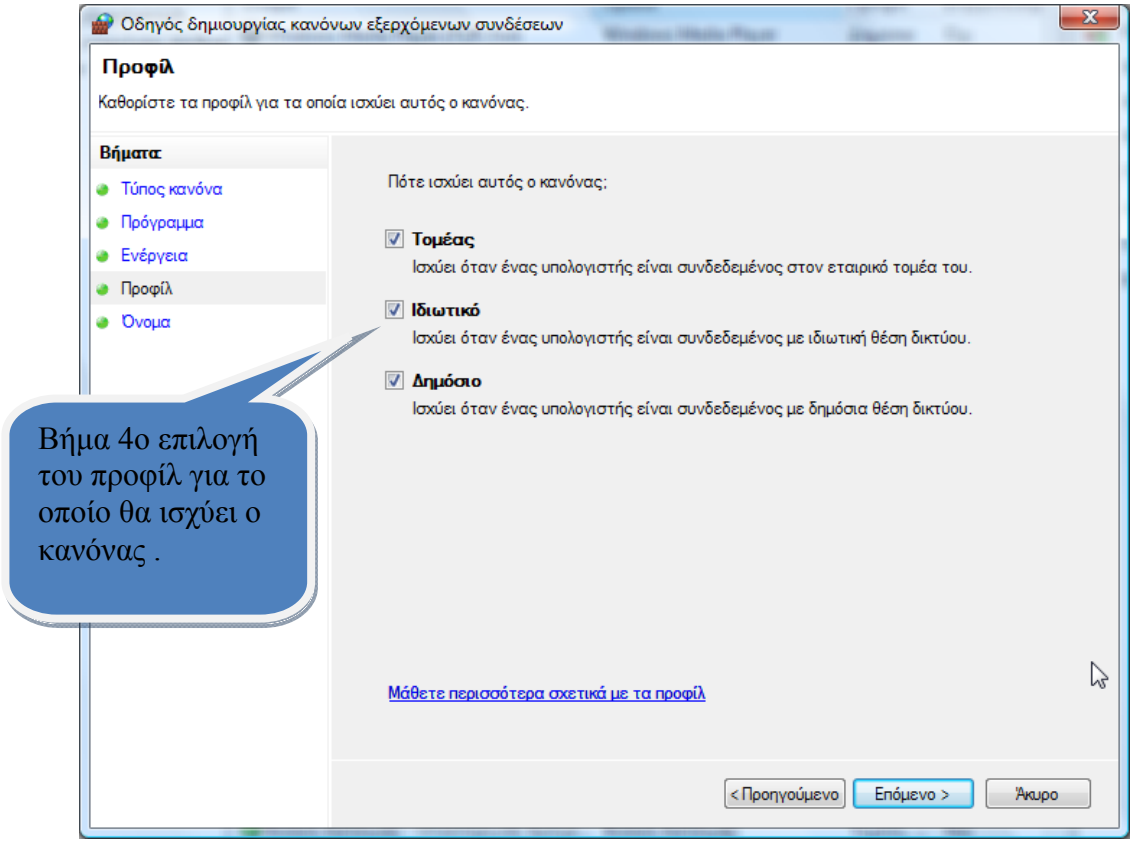
Εικόνα 22: Παράθυρο Οδηγού δημιουργίας κανόνα .



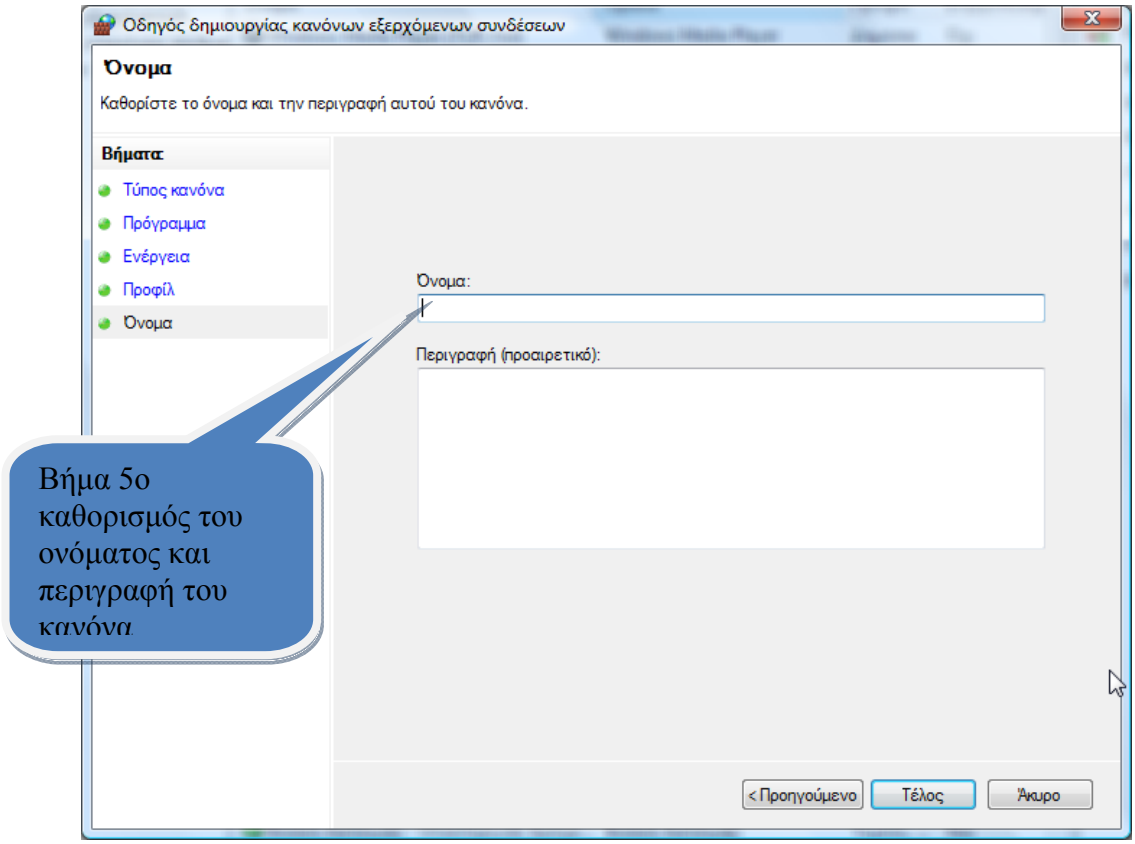
Εικόνα 23: Παράθυρο Οδηγού δημιουργίας κανόνα .



Εικόνα 24: Παράθυρο Οδηγού δημιουργίας κανόνα .



Εικόνα 25: Παράθυρο Οδηγού δημιουργίας κανόνα .



Εικόνα 26 : Παράθυρο Οδηγού δημιουργίας κανόνα .

5.1.2.5 Τι είναι το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους .

Το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους συνδυάζει ένα τείχος προστασίας κεντρικού υπολογιστή και την IPsec. Αντίθετα με ένα περιμετρικό τείχος προστασίας , το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους εκτελείται σε όλους τους υπολογιστές που λειτουργούν με την παρούσα έκδοση των Windows και παρέχει τοπική προστασία από επιθέσεις στο δίκτυο , οι οποίες μπορούν να περάσουν το περιμετρικό δίκτυο ή να δημιουργηθούν μέσα στην εταιρία μας .Επιπλέον, παρέχει ασφάλεια σύνδεσης υπολογιστή προς υπολογιστή , η οποία μας επιτρέπει να απαιτούμε έλεγχο ταυτότητας και προστασία δεδομένων κατά τις επικοινωνίες μας.

Το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους είναι ένα τείχος επίβλεψης κατάστασης που επιθεωρεί και εφαρμόζει φίλτρα σε όλα τα πακέτα κυκλοφορίας IP στις εκδόσεις 4 (IPv4) και 6 (IPv6). Από προεπιλογή , η εισερχόμενη κυκλοφορία αποκλείεται , εκτός εάν συνιστά απόκριση σε αίτημα του κεντρικού υπολογιστή (ζητούμενη κυκλοφορία) ή επιτρέπεται ρητώς (δηλαδή εάν έχει δημιουργηθεί κανόνας τείχους προστασίας που επιτρέπει την κυκλοφορία). Μπορούμε να επιτρέψουμε ρητώς την κυκλοφορία , προσδιορίζοντας έναν αριθμό θύρας , ένα

όνομα εφαρμογής , ένα όνομα υπηρεσίας, ή άλλα κριτήρια , και ρυθμίζοντας ανάλογα τις παραμέτρους του τείχους προστασίας των Windows με Ασφάλεια για προχωρημένους.

Επιπλέον, το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους μας επιτρέπει να αιτηθούμε ή να απαιτήσουμε αμοιβαίο έλεγχο ταυτότητας από τους υπολογιστές πριν την έναρξη της επικοινωνίας , καθώς και χρήση ακεραιότητας ή κρυπτογράφησης δεδομένων κατά την επικοινωνία .

5.1.2.5.1 Λειτουργία του τείχους προστασίας των Windows με Ασφάλεια για προχωρημένους .

Το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους χρησιμοποιεί δύο σύνολα κανόνων για την ρύθμιση του τρόπου ανταπόκρισης στην εισερχόμενη και εξερχόμενη κυκλοφορία . Οι κανόνες τείχους προστασίας προσδιορίζουν την κυκλοφορία που θα επιτρέπεται ή θα αποκλείεται . Οι κανόνες ασφαλείας σύνδεσης προσδιορίζουν τον τρόπο με τον οποίο θα προστατεύεται η κυκλοφορία μεταξύ του υπολογιστή μας και των άλλων υπολογιστών . Αυτοί οι κανόνες από κοινού με άλλες ρυθμίσεις , μπορούν να εφαρμόζονται με χρήση ενός προφίλ τείχους προστασίας, το οποίο ισχύει αναλόγως με το που συνδέεται ο υπολογιστής . Μπορούμε επίσης να εποπτεύουμε τις δραστηριότητες και τους κανόνες τείχους προστασίας .

5.1.2.5.2 Κανόνες τείχους προστασίας .

Μπορούμε να ρυθμίσουμε τις παραμέτρους των κανόνων τείχους προστασίας, για να καθορίσουμε εάν θα αποκλείεται ή θα επιτρέπεται η κυκλοφορία μέσα από το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους. Όταν ένα εισερχόμενο πακέτο φτάνει στον υπολογιστή μας , το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους επιθεωρεί το πακέτο και προσδιορίζει εάν πληροί τα κριτήρια που ορίζονται στον κανόνα τείχους προστασίας . Εάν το πακέτο πληροί τα κριτήρια ενός κανόνα, το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους εκτελεί την ενέργεια που καθορίζεται στον κανόνα, και αποκλείει ή επιτρέπει την σύνδεση .

Εάν το πακέτο δεν συμφωνεί με τα κριτήρια του κανόνα , το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους απορρίπτει το πακέτο και δημιουργεί μια καταχώρηση στο αρχείο καταγραφής συμβάντων του τείχους προστασίας (εάν έχει ενεργοποιηθεί η καταγραφή) . Μπορούμε να επιλέξουμε από διάφορα κριτήρια όταν ρυθμίζουμε τις παραμέτρους ενός κανόνα : Για παράδειγμα , ονόματα εφαρμογών , ονόματα υπηρεσιών συστήματος , θύρες TCP , θύρεςUDP, τοπικές διευθύνσεις IP , απομακρυσμένες διευθύνσεις IP , προφίλ, τύπους διασύνδεσης (για παράδειγμα προσαρμογέα δικτύου) ,χρήστες , ομάδες χρηστών , υπολογιστές , ομάδες υπολογιστών , πρωτόκολλα ή τύπους ICMP, και πολλά άλλα . Τα κριτήρια του κανόνα λειτουργούν προσθετικά . όσο περισσότερα κριτήρια προσθέσουμε , τόσο περισσότερο περιοριστικά αντιστοιχίζει την εισερχόμενη κυκλοφορία το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους .

5.1.2.5.3 Κανόνες ασφαλείας σύνδεσης .

Μπορούμε να χρησιμοποιήσουμε κανόνες ασφαλείας σύνδεσης για να ρυθμίσουμε τις παραμέτρους IPsec για συγκεκριμένες συνδέσεις μεταξύ αυτού του υπολογιστή και άλλων υπολογιστών . Το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους χρησιμοποιεί τον κανόνα για να αξιολογήσει την κυκλοφορία του δικτύου και μετά αποκλείει ή επιτρέπει μηνύματα με βάση τα κριτήρια που ορίζονται στον κανόνα. Υπό ορισμένες συνθήκες , το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους μπορεί να αποκλείσει την επικοινωνία. Εάν έχουμε επιλέξει μια ρύθμιση που απαιτεί ασφάλεια για μια σύνδεση (ανεξαρτήτως κατεύθυνσης) , και οι δύο υπολογιστές δεν εκτελούν μεταξύ τους έλεγχο ταυτότητας , η σύνδεση θα αποκλειστεί .

5.1.2.5.4 Προφίλ τείχους προστασίας .

Οι κανόνες τείχους προστασίας και ασφαλείας σύνδεσης , καθώς και άλλες ρυθμίσεις , μπορούν να εφαρμοστούν σε περισσότερα του ενός προφίλ τείχους προστασίας . Έπειτα αυτά τα προφίλ εφαρμόζονται στον υπολογιστή , αναλόγως με το που συνδέεται .Μπορούμε να διαμορφώσουμε ένα προφίλ για τις περιπτώσεις σύνδεσης του υπολογιστή με έναν τομέα , ένα ιδιωτικό δίκτυο , π.χ. το οικιακό δίκτυο ή ένα δημόσιο δίκτυο , π.χ. ένα Internet Cafeé .

5.1.2.5.5 Εποπτεία .

Ο κόμβος Εποπτείας εμφανίζει πληροφορίες σχετικά με τον υπολογιστή , με το οποίο είμαστε συνδεδεμένοι αυτήν την στιγμή , είτε πρόκειται για τοπικό είτε για απομακρυσμένο υπολογιστή . Αυτός ο κόμβος δεν υφίσταται εάν είμαστε συνδεδεμένοι με ένα αντικείμενο Πολιτικής ομάδας μέσω του Προγράμματος επεξεργασίας αντικειμένου Πολιτικής ομάδας .

5.1.2.5.6 Εργαλεία ρύθμισης παραμέτρων τείχους προστασίας και IPsec .

Υπάρχουν διάφοροι τρόποι για να ρυθμίσουμε τις παραμέτρου και τις επιλογές του τείχους προστασίας των Windows και της IPsec . Μερικοί από αυτούς είναι :

- **Χρήση του συμπληρωματικού προγράμματος MMC Τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους :** Το συμπληρωματικό πρόγραμμα Τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους μας επιτρέπει να ρυθμίσουμε τις παραμέτρους τόσο του τείχους προστασίας όσο και της ασφάλειας (IPsec) από ένα μόνο περιβάλλον εργασίας . Μπορούμε ακόμη να προβάλλουμε την τρέχουσα εφαρμοζόμενη πολιτική , τους κανόνες και άλλες πληροφορίες στον κόμβο Εποπτεία.

- **Χρήση του Πίνακα Ελέγχου του τείχους προστασίας των Windows :** Από τον Πίνακα Ελέγχου του τείχους προστασίας των Windows , που είναι διαθέσιμο για τον τοπικό υπολογιστή , μπορούμε να ρυθμίσουμε ένα περιορισμένο σύνολο παραμέτρων , οι οποίες

είναι διαθέσιμες μέσω του συμπληρωματικού προγράμματος της κονσόλας MMC Τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους.

- **Χρήση του συμπληρωματικού προγράμματος Πολιτικής ασφαλείας IP της κονσόλας MMC:** Αυτό το συμπληρωματικό πρόγραμμα MMC μπορεί να χρησιμοποιηθεί για τη ρύθμιση παραμέτρων των πολιτικών IPsec που εφαρμόζονται σε υπολογιστές που εκτελούν προηγούμενη έκδοση των Windows και σε υπολογιστές που αυτήν την έκδοση των Windows. Αυτό το συμπληρωματικό πρόγραμμα MMC είναι χρήσιμο για περιβάλλοντα στα οποία συνυπάρχουν υπολογιστές που λειτουργούν αυτές τις εκδόσεις των Windows .Δεν μπορούμε να χρησιμοποιήσουμε αυτό το συμπληρωματικό πρόγραμμα για να ρυθμίσουμε τις παραμέτρους του τείχους προστασίας των Windows με Ασφάλεια για προχωρημένους.

- **Χρήση του συμπληρωματικού προγράμματος Εποπτεία ασφάλειας IP της κονσόλας MMC:** Αυτό το συμπληρωματικό πρόγραμμα της κονσόλας MMC μπορεί να χρησιμοποιηθεί για την για την εποπτεία των συσχετίσεων ασφαλείας IPsec σε προηγούμενες εκδόσεις των Windows ή σε υπολογιστές που εκτελούν την παρούσα έκδοση των Windows .Το συμπληρωματικό πρόγραμμα περιλαμβάνει έναν κόμβο στατιστικών στοιχείων , ο οποίος εμφανίζει διάφορα στατιστικά στοιχεία σχετικά με τις συνδυασμένες δραστηριότητες των πολιτικών που δημιουργήθηκαν τόσο με το συμπληρωματικό πρόγραμμα Πολιτικής ασφαλείας IP όσο και με το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους.

- **Εντολές netsh:** Το netsh είναι ένα εργαλείο γραμμής εντολών , το οποίο μπορούμε να χρησιμοποιήσουμε για να ρυθμίσουμε τις παραμέτρους των στοιχείων ενός δικτύου . Το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους παρέχει το περιβάλλον **netsh advfirewall,** το οποίο μπορούμε να χρησιμοποιήσουμε για να ρυθμίσουμε τις παραμέτρους του τείχους προστασίας των Windows με Ασφάλεια για προχωρημένους . Με το netsh advfirewall , μπορούμε να δημιουργήσουμε δέσμες ενεργειών ώστε να ρυθμίζεται αυτόματα ένα σύνολο παραμέτρων του τείχους προστασίας των Windows με Ασφάλεια για προχωρημένους για την κυκλοφορία IPv4 και IPv6. Επιπλέον μπορούμε να χρησιμοποιήσουμε τις εντολές netsh advfirewall για να εμφανίσουμε τις παραμέτρους και την κατάσταση του τείχους προστασίας των Windows με Ασφάλεια για προχωρημένους.
  Μπορούμε επίσης να ρυθμίσουμε τις παραμέτρους κανόνων ασφαλείας σύνδεσης χρησιμοποιώντας τις εντολές **netsh ipsec** και να ρυθμίσουμε τις παραμέτρους πιο περιορισμένου συνόλου ρυθμίσεων τείχους προστασίας χρησιμοποιώντας τις εντολές **netsh firewall**

5.1.2.5.7 Ρυθμίσεις πολιτικής ομάδας .

Το τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους παρέχει ρυθμίσεις Πολιτικής ομάδας , τις οποίες μπορούμε να χρησιμοποιήσουμε για να ρυθμίσουμε και να διαχειριστούμε κεντρικά έναν μεγάλο αριθμό υπολογιστών ενός οργανισμού , ο οποίο χρησιμοποιεί την υπηρεσία τομέα Active Directory . Αυτές οι ρυθμίσεις Πολιτικής ομάδας μας επιτρέπουν να ρυθμίσουμε τους κανόνες του τείχους προστασίας των Windows με Ασφάλεια για προχωρημένους, καθώς και άλλα θέματα . Μπορούμε να βρούμε το συμπληρωματικό πρόγραμμα με περιήγηση στο φάκελο **Ρύθμιση παραμέτρων υπολογιστή /Ρυθμίσεις των Windows /Ρυθμίσεις ασφαλείας /Τείχος προστασίας των Windows με Ασφάλεια για προχωρημένους.**

Μπορούμε επίσης να χρησιμοποιήσουμε τα Πρότυπα διαχείρισης τείχους προστασίας των Windows για να εφαρμόσουμε ρυθμίσεις που είναι διαθέσιμες σε προηγούμενες εκδόσεις των Windows .

Τέλος , μπορούμε να χρησιμοποιήσουμε την Πολιτική ομάδας για αν ρυθμίσουμε τις παραμέτρους και να διανείμουμε πολιτικές IPsec που έχουν δημιουργηθεί με το συμπληρωματικό πρόγραμμα Πολιτικών ασφαλείας IP .

5.1.2.5.8 Τι κάνει και τι όχι το Windows Firewall των Vista.

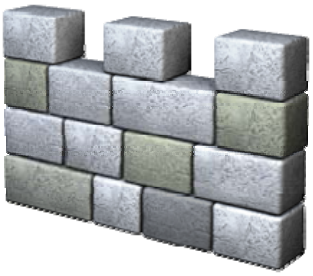
Στην παράγραφο αυτή θα αναφέρουμε επιγραμματικά τι μας προσφέρει και τι όχι το firewall των Windows Vista .
Αρχικά θα αναφέρουμε τι μας προσφέρει :

- Βοηθάει στο μπλοκάρισμα του υπολογιστή μας αποτρέποντας έτσι στους ιούς και στα worms να εκμεταλλεύονται τα μηχανήματά μας.
- Ζητάει την άδεια μας προκειμένου να μπλοκάρει ή να επιτρέπει συγκεκριμένες απαιτήσεις συνδέσεων .
- Δημιουργεί ένα αρχείο (με security log) , με τις επιτυχημένες και αποτυχημένες προσπάθειες σύνδεσης προγραμμάτων στον υπολογιστή μας . Αυτό το αρχείο μπορεί να φανεί χρήσιμο στην αντιμετώπιση προβλημάτων .

Δεν μπορεί :

- Να ανιχνεύσει ή να απενεργοποιήσει ιούς ή worms εάν αυτά βρίσκονται ήδη στον υπολογιστή μας. Για αυτόν τον λόγο θα πρέπει να επίσης να εγκαθιστούμε και κάποιο antivirus πρόγραμμα και να το κρατάμε ενημερωμένο προκειμένου να κρατάμε τον υπολογιστή μας ασφαλή .
- Να μας αποτρέψει από το να ανοίγουμε e-mail τα οποία έχουν επιβλαβή περιεχόμενο . Για αυτό θα πρέπει να είμαστε πολύ προσεχτικοί με το e-mail που ανοίγουμε και να ελέγχουμε πάντα τις επισυνάψεις αν αυτά διαθέτουν.
- Να μπλοκάρει spam ή εκούσια e-mail , από το να εμφανίζονται στα εισερχόμενα μας . Παρόλα αυτά υπάρχουν κάποια προγράμματα e-mail τα οποία μπορούν να μας βοηθήσουν σε αυτό το θέμα .

5.1.3 Windows Defender



Ο Windows Defender είναι ένα από τα νέα χαρακτηριστικά ασφάλειας των Vista γνωστό και ως **Microsoft Antispyware** . Είναι ένα πρόγραμμα λογισμικού της Microsoft το οποίο αποτρέπει , αφαιρεί καθώς και θέτει σε καραντίνα spyware στα Microsoft Windows .

Ο μηχανισμός αυτό συμπεριλαμβάνεται και είναι ενεργός εξ ορισμού στα Windows Vista , μπορεί όμως να διατεθεί και δωρεάν μέσω του Internet σε χρήστες προηγούμενων εκδόσεων των Windows όπως τα Windows XP ή Windows Server 2003.

Ο Windows Defender εκτός ότι χαρακτηρίζεται από όλες εκείνες τις ιδιότητες και τις ικανότητες που έχουν τα παρόμοια με αυτόν προγράμματα του διαδικτύου , περιλαμβάνει επιπλέον έναν μεγάλο αριθμό από πραγματικού χρόνου πράκτορες ασφαλείας οι οποίοι ελέγχουν διάφορες περιοχές των Windows προκειμένου να μην εκτεθούν και εκμεταλλευτούν από οποιοδήποτε spyware. Διαθέτει ακόμη την ικανότητα να αφαιρεί τις ActiveX εφαρμογές οι οποίες είναι εγκατεστημένες .

Τέλος ενσωματώνει την υποστήριξη του δικτύου Spy Net της Microsoft το οποίο επιτρέπει στους χρήστες να αναφέρουν στην Microsoft ότι τους απασχολεί σχετικά με τα spyware καθώς και τις εφαρμογές και τα drivers των συσκευών τα οποία επιτρέπεται να εγκατασταθούν στα συστήματα τους .

5.1.3.1 Εκδόσεις του Windows Defender

5.1.3.1.1 Έκδοση 1η του Windows Defender

Ο Windows Defender βασίζεται στο GIANT Anti Spyware , το οποίο δημιουργήθηκε από την GIANT Company Software. Η απόκτηση του προγράμματος αυτού ανακοινώθηκε από την Microsoft στις 16 Δεκεμβρίου του 2004. Ενώ το νέο αυτό πρόγραμμα υποστήριζε παλαιότερες εκδόσεις των Windows , δεν διέθετε υποστήριξη στην γραμμή των λειτουργικών συστημάτων Windows 9x .Η πρώτη έκδοση του Windows Anti Spyware κυκλοφόρησε σε έκδοση BETA στις 6 Ιανουαρίου του 2005 , και η οποία βασικά ήταν επανέκδοση του GIANT Anti Spyware.

5.1.3.1.2 Έκδοση 2η του Windows Defender

Στα μέσα του 2005 ο Bill Gates , ο κύριος αρχιτέκτονας και συνιδρυτής της Microsoft , ανακοίνωσε ότι ο Windows Defender θα παρέχεται δωρεάν σε όλες τις τελευταίες έγκυρες εκδόσεις (Windows 2000 Windows XP, Windows Server 2003 και όσες άλλες ακολουθούν), με σκοπό να τους βοηθήσει να προστατεύσουν τα μηχανήματα τους ενάντια στις συνεχώς αυξανόμενες απειλές όπως τα malware.

Ο Windows Defender έκδοση BETA 2 κυκλοφόρησε στις 13 Φεβρουαρίου του 2006. Ο κύριος πυρήνας της έκδοσης αυτής γράφτηκε σε γλώσσα προγραμματισμού C++, σε αντίθεση με το GIANT Anti Spyware το οποίο είχε γραφτεί σε γλώσσα προγραμματισμού Visual Basic . Το γεγονός αυτό βελτίωσε την επίδοση της εφαρμογής αυτής . Επίσης ,από την Beta 2 έκδοση και μετά , τα προγράμματα λειτουργούσαν ως Υπηρεσίες Windows , σε αντίθεση με τα προηγούμενες εκδόσεις , πράγμα που καθιστά την εφαρμογή αυτή ικανή να προστατεύσει τα μηχανήματα των χρηστών ακόμη και όταν οι χρήστες δεν είναι συνδεμένοι σε αυτά .

Η έκδοση αυτή απαιτεί την πιστοποίηση του Windows Genuine Advantage . Παρόλα αυτά δεν περιέχει μερικά από τα εργαλεία που μπορούσαμε να βρούμε στη Beta 1 έκδοση . Η Microsoft αφαίρεσε τα παρακάτω εργαλεία: System Inoculation, Secure Shredder και System Explorer τα οποία εργαλεία μπορούσαμε να βρούμε στην προηγούμενη έκδοση, επίσης δεν υπάρχει και το εργαλείο Tracks Eraser το οποίο επιτρέπει στους χρήστες να σβήσουν εύκολα διάφορων τύπων προσωρινά αρχεία τα οποία σχετίζονται με τον Internet Explorer συμπεριλαμβανομένων των cookies, των temporary internet files και του Windows Media Player playback history

5.1.3.1.3 Τελική έκδοση του Windows Defender

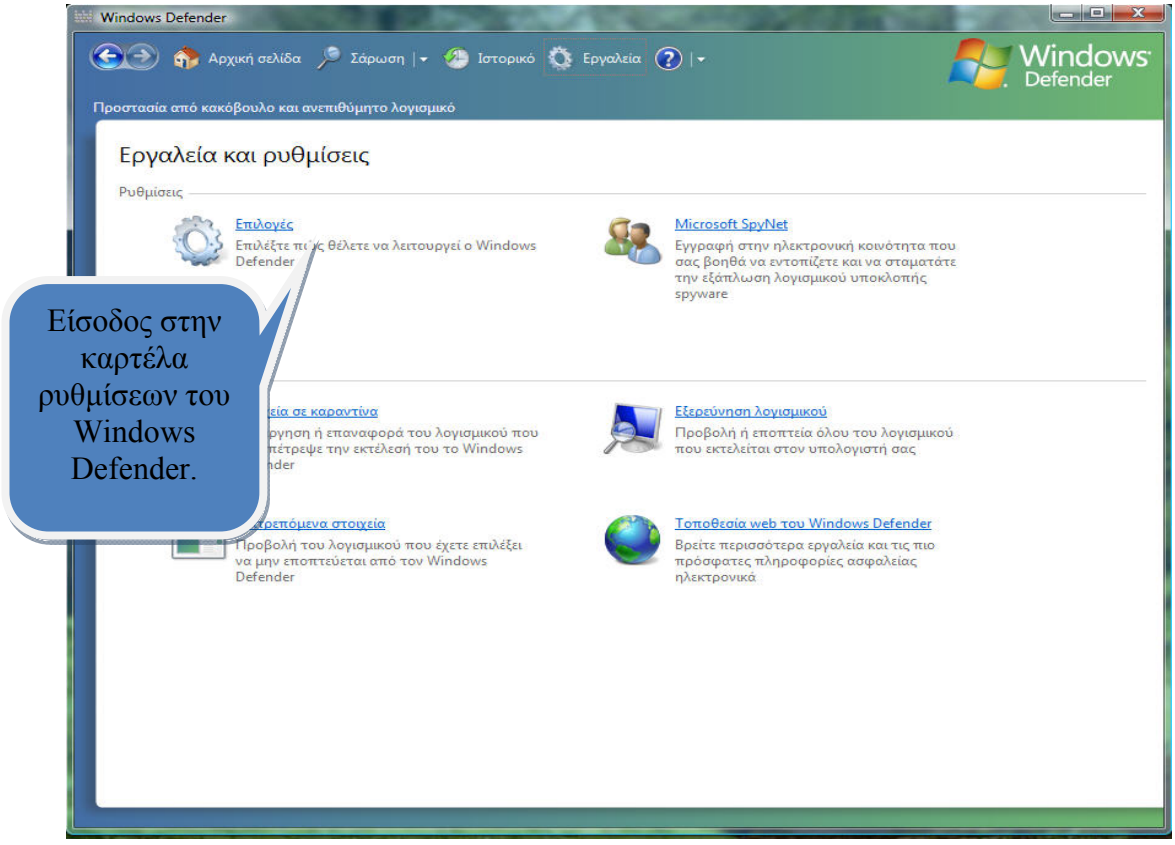
Η τελική έκδοση του Windows Defender κυκλοφόρησε στις 24 Οκτωβρίου του 2006, υποστηρίζει τις εκδόσεις των Windows XP,Server 2003 και Vista , παρόλα αυτά σε αντίθεση με τις Beta εκδόσεις δεν τρέχει η έκδοση αυτής στα Windows 2000 .

5.1.3.2 Περιγραφή του Windows Defender

Αρχικό παράθυρο του Windows Defender.

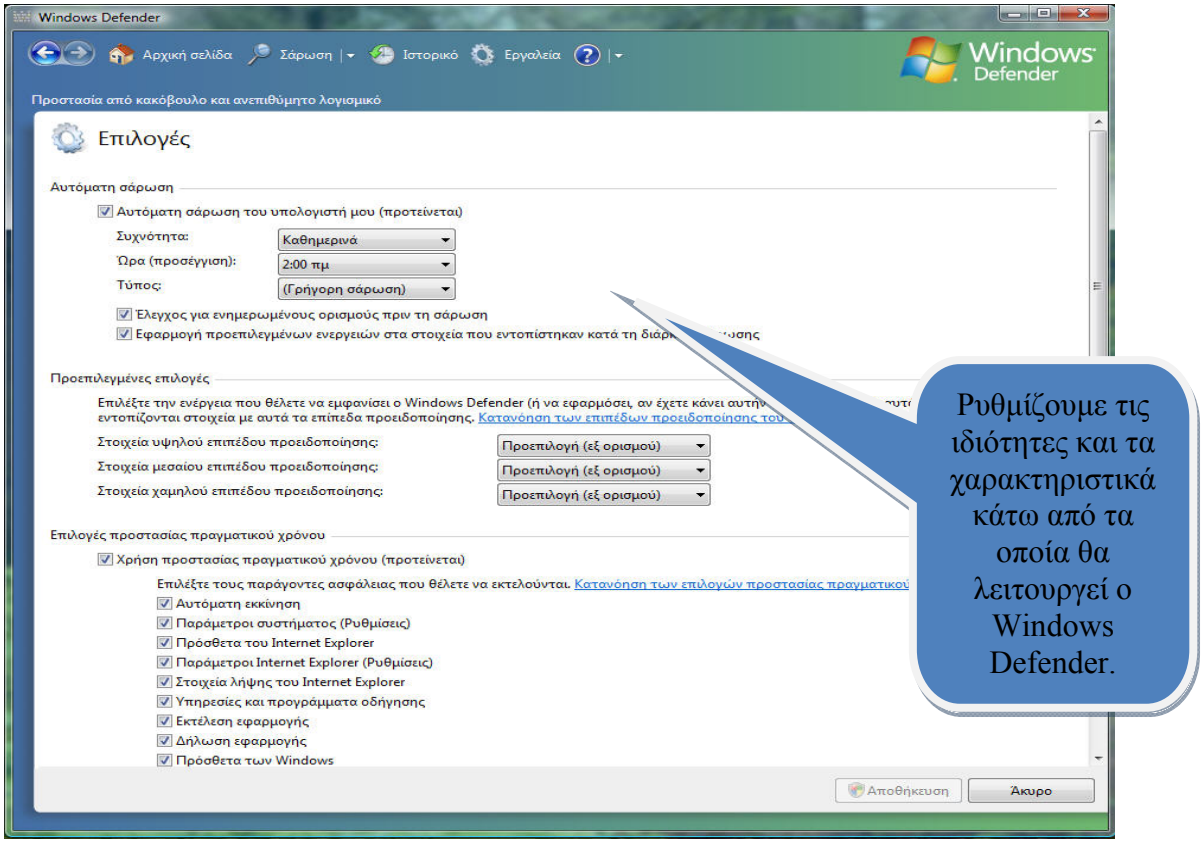
Το παράθυρο αυτό εμφανίζεται την πρώτη φορά που θέτουμε σε λειτουργία τον Windows Defender. Στο σημείο αυτό μπορούμε να ρυθμίσουμε τις ιδιότητες του μηχανισμού αυτού .

Στη συνέχεια και αφού ρυθμίσουμε και αποθηκεύσουμε τις επιλογές μας ,κάθε φορά που θα εκτελούμε τον Windows Defender το παράθυρο που θα ανοίγει θα είναι αυτό της αρχικής σελίδας του Windows Defender.



Εικόνα 27: Αρχικό παράθυρο του Windows Defender των Windows .

Παράθυρο Εργαλεία του Windows Defender



Εικόνα 28 : Παράθυρο Εργαλεία του Windows Defender των Windows .

Στην καρτέλα αυτή καθορίζουμε τα χαρακτηριστικά γνωρίσματα και τις ιδιότητες με τις οποίες θα λειτουργεί ο Windows Defender .

Αρχικά εμφανίζονται οι επιλογές των Αυτόματων λειτουργιών. Όπως :

- Η ενεργοποίηση ή όχι της αυτόματης σάρωσης του υπολογιστή .
- Συχνότητα σάρωσης (Κάθε πότε θα εκτελείται δηλαδή η σάρωση).
- Ώρα (τι ώρα θα πραγματοποιείται η σάρωση).
- Τύπος (τι είδους σάρωση θα εκτελείται : Γρήγορη, Πλήρης , Προσαρμοσμένη).
- Έλεγχος ενημερώσεων (Να γίνεται δηλαδή αναζήτηση ενημερώσεων πριν την σάρωση ή όχι)
- Εφαρμογή ενεργειών που έχουμε ορίσει στα κακόβουλα στοιχεία που εντοπίστηκαν κατά την σάρωση .

Στο δεύτερο κομμάτι των ρυθμίσεων , εμφανίζονται οι επιλογές που αφορούν τις ενέργειες που θα επιβάλλονται σε περίπτωση ανίχνευσης κακόβουλου λογισμικού .

Οι επιλογές σε αυτό το κομμάτι είναι οι ακόλουθες:

- Στοιχεία Υψηλού επιπέδου προειδοποίησης : Εδώ δηλαδή επιλέγουμε ,όταν ανιχνευτεί ένα υψηλού επιπέδου στοιχείο , τι ενέργεια θα εκτελεστεί : Ειδοποίηση, Παράβλεψη , Κατάργηση. Εξ ορισμού είναι επιλεγμένη η Ειδοποίηση .
- Στοιχεία Μεσαίου επιπέδου προειδοποίησης : Ομοίως και εδώ επιλέγουμε μια από τις ίδιες ενέργειες , Ειδοποίηση, Παράβλεψη , Κατάργηση οι οποίες θα εκτελούνται σε περίπτωση ανίχνευσης μεσαίου επιπέδου στοιχείου .
- Στοιχεία Χαμηλού επιπέδου προειδοποίησης :Τέλος και στην τρίτη αυτή ρύθμιση επιλέγουμε ομοίως μια από τις τρείς ενέργειες που προαναφέραμε και η οποία θα εκτελείται σε περίπτωση ανίχνευσης χαμηλού επιπέδου στοιχείου.

Του επόμενου κομματιού οι ρυθμίσεις , αφορούν τις επιλογές προστασίας πραγματικού χρόνου.

Όταν αναφερόμαστε στην προστασία πραγματικού χρόνου , εννοούμε τις προειδοποιήσεις που θα δεχόμαστε άμεσα μετά τον εντοπισμό κάποιου λογισμικού υποκλοπής Spyware και γενικά οποιοδήποτε ανεπιθύμητο λογισμικό που ίσως επιχειρήσει να εγκατασταθεί ή να εκτελεστεί στον υπολογιστή μας .

Όπως και στην προηγούμενη περίπτωση έτσι και εδώ ανάλογα με το επίπεδο προειδοποίησης , μπορούμε να επιλέξουμε και αντίστοιχη ενέργεια αντιμετώπισης (Παράβλεψη, Καραντίνα, Αφαίρεση , Να επιτρέπεται πάντα). Οι επιλογές που έχουμε διαθέσιμες στο κομμάτι αυτό είναι οι ακόλουθες :

- Χρήση ή όχι της προστασίας πραγματικού χρόνου
- Επιλογή των παραγόντων ασφάλειας που θα εκτελούνται (Αυτόματη εκκίνηση, Παράμετροι συστήματος , Πρόσθετα του Internet Explorer,κ.α.)
- Επιλογή του αν ο Windows Defender πρέπει να μας ειδοποιεί ή όχι κάποιες καταστάσεις , όπως για λογισμικό του οποίου οι κίνδυνοι δεν είναι ακόμη γνωστοί ή ακόμη για αλλαγές που έγιναν στον υπολογιστή μας από λογισμικό του οποίου έχουμε επιτρέψει την εκτέλεση του .
- Επιλογή του πότε θα εμφανίζεται το εικονίδιο του Windows Defender στην περιοχή ειδοποίησης ,(πάντα ή μόνο σε περιπτώσεις που λόγω κάποιας επιμέρους ενέργειας ο Windows Defender πρέπει να εκτελεστεί).

Στο τελευταίο κομμάτι των ρυθμίσεων βρίσκονται οι ρυθμίσεις για προχωρημένους . Οι ρυθμίσεις αυτές αναφέρονται σε εξειδικευμένες επιλογές όπως :

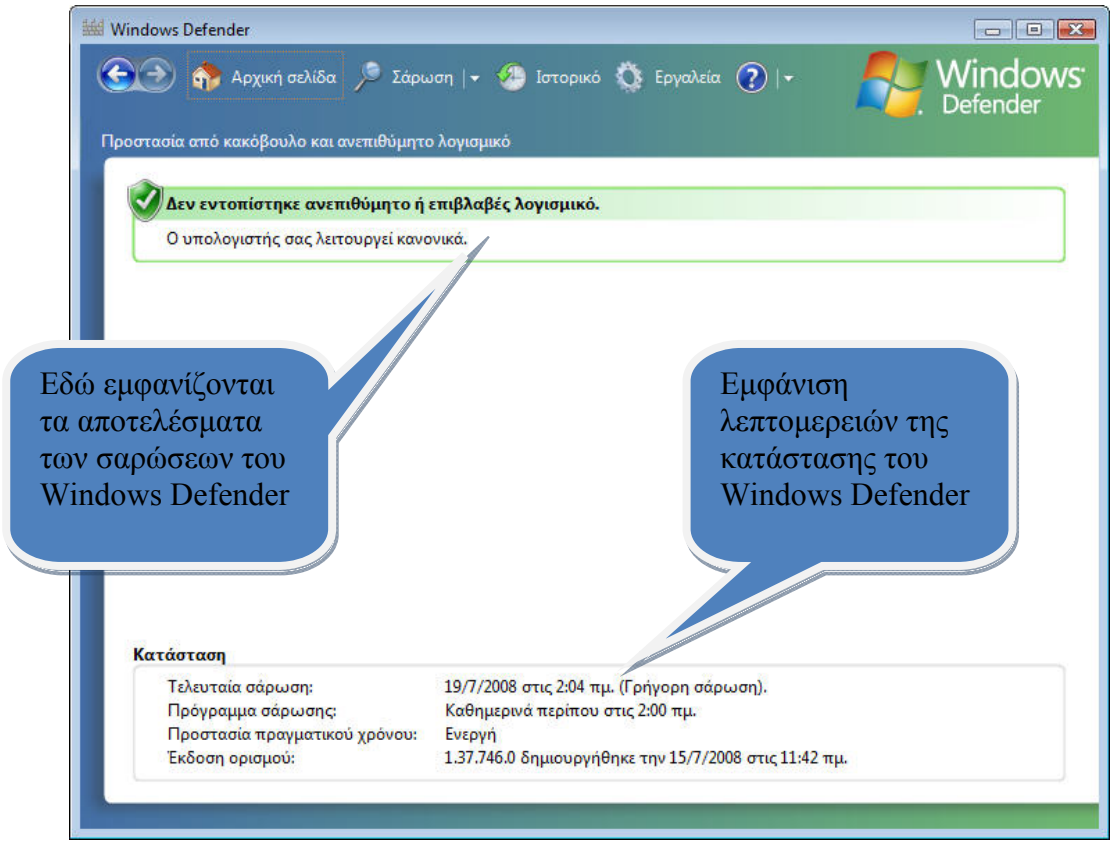
- Σάρωση των περιεχομένων των αρχειοθετημένων αρχείων και φακέλων για πιθανές απειλές .
- Χρήση ευρετικών ,για εντοπισμό επιβλαβούς ή ανεπιθύμητου λογισμικού που δεν έχει αναλυθεί για κινδύνους .

- Δημιουργία σημείου επαναφοράς πριν την εφαρμογή ενεργειών στα στοιχεία που εντοπίστηκαν .
- Χρήση του Windows Defender.
- Να επιτρέπεται σε όλους η χρήση του Windows Defender.

Παράθυρο Αρχική σελίδα του Windows Defender

Στο παράθυρο αυτό εμφανίζονται τα αποτελέσματα ,όσο αφορά την εμφάνιση κακόβουλων λογισμικών , μετά την ολοκλήρωση κάποιας σάρωσης . Εάν έχει ολοκληρωθεί η σάρωση και δεν έχει ανευρεθεί κανένα επιβλαβές λογισμικό , εμφανίζεται ένα αντίστοιχο μήνυμα σαν αυτό που εμφανίζεται στο παρακάτω παράθυρο .

Στο παράθυρο αυτό εμφανίζονται ακόμη λεπτομέρειες για όσο αφορά την κατάσταση του Windows Defender. Όπως για το πότε έγινε η τελευταία σάρωση , κάθε πότε εκτελείται το πρόγραμμα της σάρωσης , αν είναι ενεργή ή όχι η προστασία πραγματικού χρόνου κ.α.



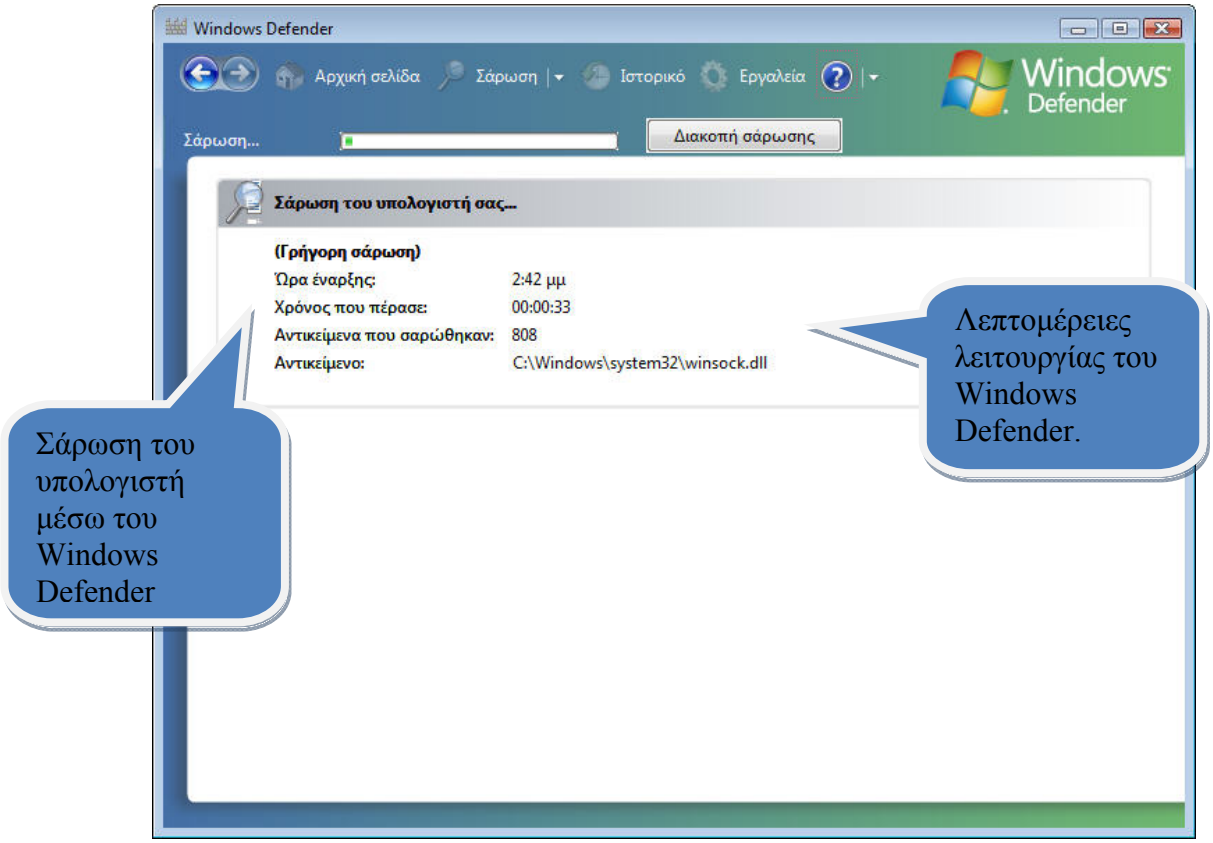
Εικόνα 29: Παράθυρο Αρχική σελίδα του Windows Defender των Windows .

Παράθυρο Σάρωση του Windows Defender

Στο παράθυρο αυτό μπορούμε να θέσουμε άμεσα σε λειτουργία τον Windows Defender . Ο Windows Defender στην ουσία είναι ένα antivirus των Windows , το οποίο αντιδρά όμοια με οποιοδήποτε άλλο antivirus τρίτων κατασκευαστών .

Εντοπίζει , ειδοποιεί και αντιμετωπίζει με οποιονδήποτε τρόπο εμείς του υποδείξουμε την ¨ πληγή¨ που θα ανιχνεύσει στο σύστημα μας .

Στο κεντρικό μέρος του παραθύρου αυτού εμφανίζονται λεπτομέρειες σχετικές με σάρωση που εκτελείται εκείνη την χρονική στιγμή . Οι λεπτομέρειες αυτές αφορούν την ώρα έναρξης της σάρωσης αυτής , τον χρόνο που εκτελείται η σάρωση , πόσα αντικείμενα έχουν σαρωθεί μέχρι στιγμής και τέλος στο σημείο με την επικεφαλίδα αντικείμενο εμφανίζεται το μονοπάτι του αντικειμένου το οποίο σαρώνεται εκείνη την στιγμή από τον Windows Defender.



Εικόνα 30 : Παράθυρο Σάρωσης του Windows Defender των Windows .

5.1.3.2.1 Προβολή της προόδου μιας σάρωσης του Windows Defender .

Μέσω του προαναφερθέντος παραθύρου του Windows Defender , μπορούμε να δούμε ποιός τύπος σάρωσης του Windows Defender βρίσκεται σε εξέλιξη και να δούμε ακόμη για πόσο χρόνο εκτελείται μέχρι στιγμής .

Προβολή της προόδου μιας σάρωσης :

1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender** .

2. Αν υπάρχει σάρωση σε εξέλιξη , η πρόοδος προβάλλεται ωσότου ολοκληρωθεί η σάρωση . Αν η σάρωση έχει ολοκληρωθεί , η κατάσταση θα προβάλλει τα αποτελέσματα της σάρωσης και την ημερομηνία και την ώρα που ολοκληρώθηκε η σάρωση .

5.1.3.2.2 Προγραμματίζουμε πότε ο Windows Defender θα εκτελεί σάρωση του υπολογιστή μας .

Επειδή η σάρωση του υπολογιστή μας είναι αναγκαία σε καθημερινή βάση οι δημιουργοί μας συνιστούν να προγραμματίσουμε έτσι τον υπολογιστή μας , έτσι ώστε να εκτελεί μια καθημερινή γρήγορη σάρωση . Η γρήγορη σάρωση θα ελέγχει τις περιοχές του υπολογιστή μας τις οποίες είναι πιθανότερο να προσβάλλει λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό.
Σε περίπτωση τώρα που επιθυμούμε το Windows Defender να ελέγξει όλα τα αρχεία και τα προγράμματα στον υπολογιστή μας το ρυθμίζουμε έτσι ώστε να εκτελεί μια πλήρη σάρωση .

Για να ενισχύσουμε την ασφάλεια του υπολογιστή μας , μπορούμε ακόμη να επιλέξουμε να καταργήσουμε αυτόματα το λογισμικό υποκλοπής spyware ή άλλο πιθανώς ανεπιθύμητο λογισμικό που θα ανιχνευτεί κατά την διάρκεια της σάρωσης .

Τα βήματα που ακολουθούμε προκειμένου να προγραμματίσουμε το Windows Defender είναι τα ακόλουθα :

1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender**.

2. Κάνουμε κλικ στο μενού **Εργαλεία** και στην συνέχεια κάνουμε κλικ στην εντολή **Επιλογές**.

3. Στην επιλογή **Αυτόματη σάρωση** επιλέγουμε το πλαίσιο επιλογής **Αυτόματη σάρωση του υπολογιστή μου (προτείνεται)** , στην συνέχεια επιλέγουμε την συχνότητα , την ώρα της ημέρας και τον τύπο της σάρωσης που θέλουμε να εκτελείται .

4. Για να αφαιρείται αυτόματα το λογισμικό υποκλοπής spyware ή άλλο πιθανώς ανεπιθύμητο λογισμικό μετά από την σάρωση , επιλέγουμε το πλαίσιο ελέγχου **Εφαρμογή προεπιλεγμένων ενεργειών στα στοιχεία που εντοπίστηκαν κατά την σάρωση** .

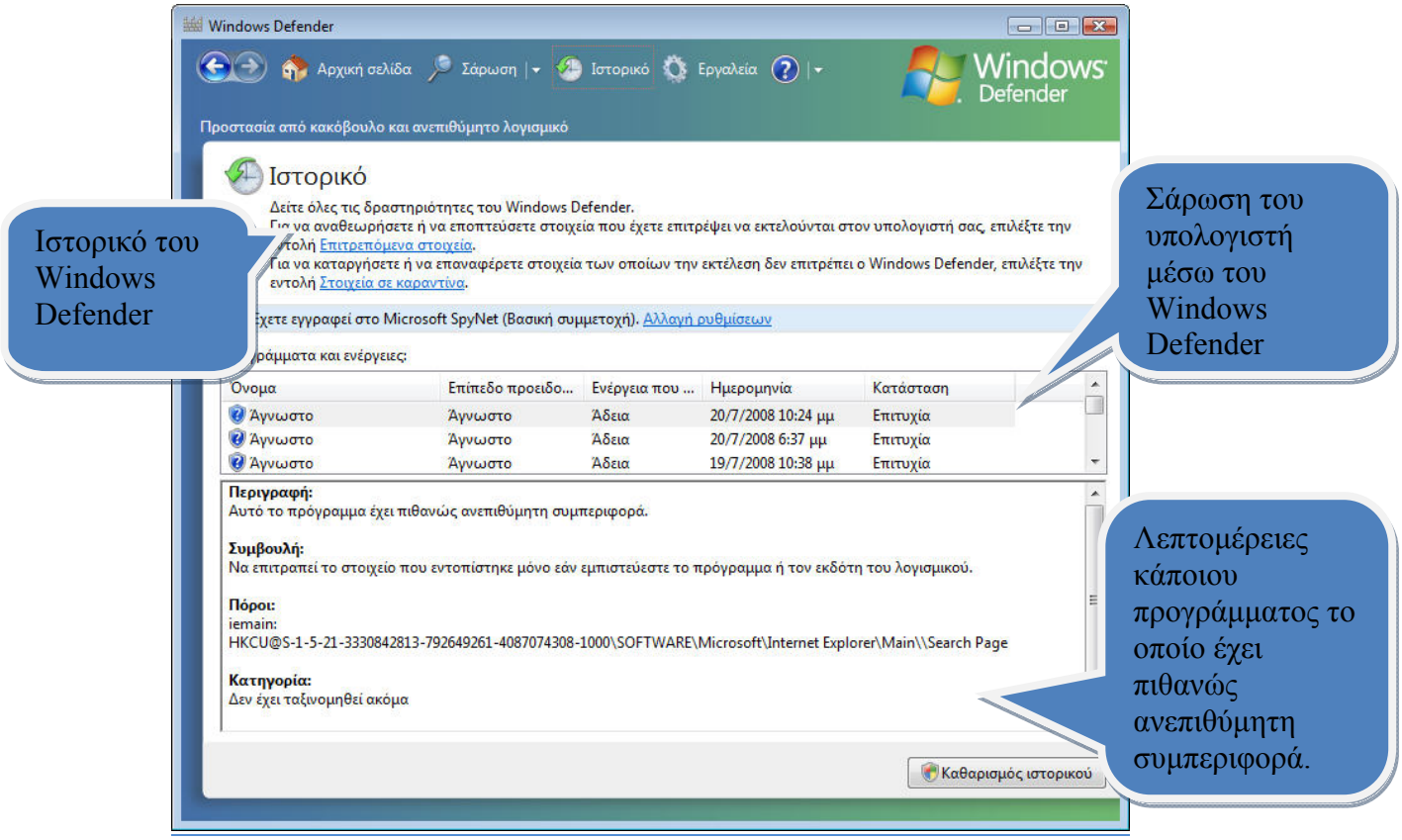
5. Στην επιλογή **Προεπιλεγμένες ενέργειες** , επιλέγουμε την ενέργεια που θέλουμε να εκτελείται σε κάθε προειδοποίηση του Windows Defender και κάνουμε κλικ στο κουμπί **Αποθήκευση** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση .

Παράθυρο Ιστορικό του Windows Defender

Στο παράθυρο του Ιστορικού , μπορούμε να δούμε όλες τις δραστηριότητες στις οποίες έχει προβεί ο Windows Defender τον τελευταίο καιρό.

Από το παράθυρο αυτό μας δίνεται η δυνατότητα , μέσω διαφόρων συνδέσεων , να αναθεωρήσουμε ή να εποπτεύσουμε στοιχεία που έχουμε επιτρέψει να εκτελούνται στον υπολογιστή μας, ακόμη μπορούμε να καταργήσουμε ή να επαναφέρουμε στοιχεία των οποίων η εκτέλεση δεν επιτρέπει ο Windows Defender.

Στο κεντρικό κομμάτι του παραθύρου αυτού παρακολουθούμε λεπτομέρειες προγραμμάτων και ενεργειών , που τους έχει χορηγηθεί η πρόκειται να τους χορηγηθεί ή ακόμη και να τους απαγορευτεί κάποιου είδους άδεια.



Εικόνα 31 : Παράθυρο Ιστορικού του Windows Defender των Windows .

5.1.3.2.3 Προβολή ή απαλοιφή του ιστορικού του Windows Defender.

Το ιστορικό του Windows Defender , προβάλλει τις ενέργειες που έχουν εφαρμοστεί στο λογισμικό υποκλοπής spyware ή άλλο πιθανώς ανεπιθύμητο λογισμικό που ανίχνευσε στον υπολογιστή μας το Windows Defender .

Οι ενέργειες που ακολουθούμε προκειμένου να επεξεργαστούμε το ιστορικό είναι οι ακόλουθες :

1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender**.
2. Κάνουμε κλικ στο **Ιστορικό**.
3. Για να διαγράψουμε όλα τα στοιχεία της λίστας , κάνουμε κλικ στο **Καθαρισμός ιστορικού** , αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση .

5.1.3.2.4 Διατήρηση ενημερωμένων ορισμών του Windows Defender.

Οι ορισμοί του Windows Defender , είναι αρχεία που λειτουργούν ως εγκυκλοπαίδεια γνωστού λογισμικού υποκλοπής spyware ή άλλου πιθανώς ανεπιθύμητου λογισμικού . Επειδή το λογισμικό υποκλοπής spyware αναπτύσσεται συνεχώς το Windows Defender βασίζεται στους ενημερωμένους ορισμούς προκειμένου να καθορίσει εάν το λογισμικό που επιχειρεί να εγκατασταθεί , να εκτελεστεί ή να αλλάξει τις ρυθμίσεις του υπολογιστή μας είναι πιθανώς ανεπιθύμητο ή κακόβουλο .

Το Windows Defender συνεργάζεται με τις ρυθμίσεις του Windows Update για να εγκαθιστά αυτόματα τους πιο πρόσφατους ορισμούς . Παρόλα αυτά μπορούμε και εμείς σαν απλοί χρήστες να ελέγξουμε είτε αυτόματα είτε μη αυτόματα για νέους ορισμούς :

- **Αυτόματος έλεγχος για νέους ορισμούς πριν από τις προγραμματισμένες σαρώσεις (προτείνεται)** .

    1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender**.
    2. Κάνουμε κλικ στο μενού **Εργαλεία** και στην συνέχεια κάνουμε κλικ στην εντολή **Επιλογές**.
    3. Στην επιλογή **Αυτόματη σάρωση** επιλέγουμε το πλαίσιο επιλογής **Αυτόματη σάρωση του υπολογιστή μου (προτείνεται)** .
    4. Επιλέγουμε το πλαίσιο ελέγχου **Έλεγχος για ενημερωμένους ορισμούς πριν την σάρωση** και έπειτα κάνουμε κλικ στο **Αποθήκευση** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση .

- **Μη αυτόματος έλεγχος για νέους ορισμούς .**

    1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender**.
    2. Κάνουμε κλικ στο βέλος δίπλα στο κουμπί **¨Βοήθεια ¨** και μετά κάνουμε κλικ στην επιλογή **Έλεγχος για ενημερώσεις** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση .

5.1.3.2.5 Κατάργηση του λογισμικού υποκλοπής spyware από τον υπολογιστή μας .

Το λογισμικό υποκλοπής spyware συχνά μπορεί να μολύνει περιοχές του υπολογιστή μας που είναι δύσκολο να καθαριστούν , χωρίς να προκληθούν άλλα προβλήματα . Αν κάποιο πρόγραμμα

προστασίας από υποκλοπές μας ενημερώσει ότι δεν μπορεί να αφαιρέσει το λογισμικό υποκλοπής , ακολουθούμε τις οδηγίες που μας παρέχει το πρόγραμμα . Αν αυτό δεν λειτουργήσει , δοκιμάζουμε ένα από ακόλουθα βήματα :

- Ελέγχουμε τα **Εγκαταστημένα προγράμματα** για στοιχεία που δεν ανήκουν στον υπολογιστή μας . Χρησιμοποιούμε αυτήν την μέθοδο με πολύ μεγάλη προσοχή . Ο Πίνακάς Ελέγχου αναφέρει πολλά προγράμματα τα περισσότερα από τα οποία δεν είναι λογισμικό υποκλοπής spyware . Πολλά προγράμματα υποκλοπής spyware χρησιμοποιούν ειδικές μεθόδους εγκατάστασης , προκειμένου να μην εμφανίζονται στα ¨Εγκατεστημένα προγράμματα¨ . Μερικές φορές , κάποιο πρόγραμμα λογισμικού υποκλοπής spyware διαθέτει επιλογή απεγκατάστασης και μπορεί να καταργηθεί με αυτήν την μέθοδο . Είναι χρήσιμο να καταργούμε τα προγράμματα που μπορούμε να αναγνωρίσουμε με βεβαιότητα ως λογισμικό υποκλοπής spyware και να μην καταργούμε τα προγράμματα που ίσως θέλουμε να κρατήσουμε , ακόμη και αν δεν τα χρησιμοποιούμε πολύ συχνά .

- Να εγκαταστήσουμε ξανά τα Windows .
  Ορισμένες εφαρμογές υποκλοπής spyware μπορούν να κρυφτούν τόσο καλά ‘ώστε να είναι αδύνατον να καταργηθούν . Αν εξακολουθούμε να έχουμε ενδείξεις ότι υπάρχει κάποιο λογισμικό υποκλοπής spyware , αφού επιχειρήσουμε να το καταργήσουμε με κάποιο πρόγραμμα προστασίας από λογισμικά υποκλοπής ή να το απεγκαταστήσουμε , ίσως χρειαστεί να επανεγκαταστήσουμε τα Windows και τα προγράμματά μας .

5.1.3.3 Τι κάνει ο Windows Defender.

Ο Windows Defender είναι ένα λογισμικό το οποίο βοηθάει στο να προστατεύσουμε τα μηχανήματα μας από τα pop-ups , την μείωση της απόδοσής τους ή από τις απειλές ασφαλείας οι οποίες προκαλούνται από τα spyware και τα άλλα κακόβουλα λογισμικά . Η προστασία αυτή παρέχεται με το να ανιχνεύονται και να αφαιρούνται τα γνωστά spyware από τους υπολογιστές μας .

Τα χαρακτηριστικά του Windows Defender είναι η πραγματικού χρόνου προστασία , ένα σύστημα ελέγχου το οποίο συνιστά πράξεις κατά των spyware όταν αυτά ανιχνεύονται , μείωση των διακοπών καθώς και άλλου τύπου βοήθειες οι οποίες μας καθιστούν παραγωγικούς .

Τα πλεονεκτήματα της εγκατάστασης του Windows Defender είναι :

- Μπορεί εύκολα και γρήγορα να βρίσκει τα spyware και τα άλλα κακόβουλα λογισμικά , να εμφανίζει τα ενοχλητικά pop-up ads , τις αλλαγές στις ρυθμίσεις του Internet Explorer , ή ακόμη και την χρήση των προσωπικών μας δεδομένων χωρίς την συγκατάθεσή μας .

- Αποβάλλει τα ανιχνευόμενα και προς εμάς κατευθυνόμενα spyware , καθώς και αν ακούσια αφαιρέσουμε κάποιο πρόγραμμα το οποίο στην πραγματικότητα το χρειαζόμαστε , μας βοηθάει εύκολα να το ανακτήσουμε .

- Μας επιτρέπει να προγραμματίσουμε τους χρόνους ανίχνευσης και αφαίρεσης των κακόβουλων λογισμικών όποτε χρονικά μας βολεύει σε όποιο πρόγραμμα επιθυμούμε .

- Παρέχει βελτιωμένη και πιο ασφαλή περιήγηση στο Internet . Ο Windows Defender βοηθάει εμποδίζοντας τα spyware προτού αυτά διεισδύσουν στον υπολογιστή μας . Ο Windows Defender επίσης μας προσφέρει μια συνεχής προστασία σχεδιασμένη με σκοπό να στοχεύει σε όλους τους τρόπους διεισδύσεων των spyware στα συστήματα μας .

- Ο Windows Defender λειτουργεί χωρίς να μας ¨ενοχλεί¨. Τρέχει στο background και διαχειρίζεται οποιαδήποτε επίθεση spyware και αν αντιμετωπίσει με βάση τις ρυθμίσεις και τις προτιμήσεις που εμείς του έχουμε προσδιορίσει . Χρησιμοποιεί έτσι τον υπολογιστή μας με την ελάχιστη προς εμάς διακοπή .

- Συνεχώς ανανεώνεται και μια ομάδα ερευνητών της Microsoft ψάχνει διαρκώς στο Διαδίκτυο για να ανακαλύψει οποιοδήποτε νέο είδος spyware και να αναπτύξει ανάλογες μεθόδους αντίδρασης προς αυτό .

- Διαθέτει ένα εθελοντικό παγκόσμιο δίκτυο χρηστών υπερασπιστών των Windows οι οποίοι βοηθούν την Microsoft να καθορίσει ποια ύποπτα προγράμματα μπορούν να ταξινομηθούν ως spyware. Η βοήθεια αυτών των συμμετασχόντων ανακαλύπτει τις νέες απειλές γρήγορα και ειδοποιεί τους αναλυτές της Microsoft , έτσι ώστε ο καθένας να μπορεί να προστατεύεται καλύτερα . Κάθε χρήστης μπορεί να ενωθεί σε αυτό το δίκτυο και να βοηθήσει και αυτός από την μεριά του δημιουργώντας τέτοιου είδους εκθέσεις .

5.1.3.4 Χρήση του Windows Defender.

Ο Windows Defender είναι ένα πολύ χρήσιμο εργαλείο το οποίο συνιστάται να το χρησιμοποιούμε σε καθημερινή βάση και γενικά όποτε χρησιμοποιούμε τον υπολογιστή μας για καλύτερη δική μας προστασία .
Ο βασικός λόγος είναι ότι το λογισμικό υποκλοπής spyware καθώς και οποιοδήποτε άλλο πιθανώς ανεπιθύμητο λογισμικό μπορεί να επιχειρεί να εγκατασταθεί στον υπολογιστή μας κάθε φορά που συνδεόμαστε στο Internet .Μπορούν επίσης να μολύνουν τον υπολογιστή μας όταν εγκαθιστάμε ορισμένα προγράμματα χρησιμοποιώντας ένα CD ή DVD ή κάποιο άλλο αφαιρούμενο μέσο . Το πιθανώς ανεπιθύμητο ή κακόβουλο λογισμικό , μπορεί επίσης να προγραμματιστεί να εκτελείται απρόσμενα και όχι μόνον όταν εγκατασταθεί .

Το Windows Defender προσφέρει τρείς τρόπους για να αποφεύγεται η μόλυνση του υπολογιστή μας από λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό :

- **Προστασία σε πραγματικό χρόνο :** Το Windows Defender μας προειδοποιεί όταν κάποιο λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό επιχειρήσει να εγκατασταθεί ή να εκτελεστεί στον υπολογιστή μας .Επίσης μας προειδοποιεί όταν κάποια προγράμματα επιχειρήσουν να αλλάξουν σημαντικές ρυθμίσεις των Windows .

- **Κοινότητα Spy Net:** Η διαδικτυακή κοινότητα Microsoft Spy Net μας βοηθά να βλέπουμε τις αντιδράσεις των άλλων στο λογισμικό που δεν έχει ακόμη ταξινομηθεί αναφορικά με τον κίνδυνο που ενέχει . Το να παρακολουθούμε εάν τα άλλα μέλη της κοινότητας επιτρέπουν την λειτουργία κάποιου λογισμικού μας βοηθά να επιλέξουμε εάν θα επιτρέψουμε σε αυτό να εγκατασταθεί στον υπολογιστή μας . Και οι δικές μας επιλογές , εφόσον συμμετέχουμε, μπορούν να προστεθούν στις αξιολογήσεις της κοινότητας , για να βοηθηθούν οι άλλοι χρήστες να λάβουν τα κατάλληλα μέτρα .

- **Επιλογές σάρωσης :** Μπορούμε να χρησιμοποιήσουμε τον Windows Defender για να εκτελέσουμε σάρωση για το λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό στον υπολογιστή μας , για να προγραμματίσουμε τις τακτικές σαρώσεις και για να καταργήσουμε αυτόματα το κακόβουλο λογισμικό που ανιχνεύεται από την σάρωση .

Όταν χρησιμοποιούμε τον το Windows Defender , είναι σημαντικό να έχουμε ενημερωμένους ορισμούς . Οι ορισμοί είναι αρχεία που λειτουργούν σαν συνεχώς αναπτυσσόμενη εγκυκλοπαίδεια ενδεχόμενων απειλών λογισμικού . Το Windows Defender χρησιμοποιεί ορισμούς για να προσδιορίσει εάν το λογισμικό που ανιχνεύεται είναι spyware ή άλλο πιθανώς ανεπιθύμητο λογισμικό και έπειτα μας προειδοποιεί για τους ενδεχόμενους κινδύνους . Για να διατηρήσουμε τους ορισμούς ενημερωμένους , το Windows Defender συνεργάζεται με την τοποθεσία web Windows Update για την αυτόματη εγκατάσταση νέων ορισμών , μόλις αυτοί δημοσιευθούν .Μπορούμε ακόμη να ορίσουμε στον Windows Defender να ελέγχει στο Internet για ενημερωμένους ορισμούς πριν την σάρωση .

5.1.3.5 Κατανόηση της προστασίας σε πραγματικό χρόνο .

Η προστασία σε πραγματικό χρόνο μας προειδοποιεί όταν κάποιο λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό επιχειρεί να εγκατασταθεί ή να εκτελεστεί στον υπολογιστή μας. Ανάλογα με το επίπεδο προειδοποίησης , μπορούμε να επιλέξουμε μια από τις παρακάτω ενέργειες για να εφαρμοστεί στο λογισμικό :

- **Παράβλεψη .** Επιτρέπει την εγκατάσταση ή την λειτουργία του λογισμικού στον υπολογιστή μας . Αν το λογισμικό εξακολουθεί να λειτουργεί κατά την επόμενη σάρωση ή εάν το λογισμικό επιχειρήσει να αλλάξει ρυθμίσεις του υπολογιστή μας που σχετίζονται με την ασφάλεια , το Windows Defender θα μας προειδοποιήσει και πάλι σχετικά με το λογισμικό αυτό

- **Καραντίνα.** Όταν το Windows Defender τοποθετήσει λογισμικό σε καραντίνα , το μετακινεί σε κάποια άλλη τοποθεσία στον υπολογιστή μας και , στην συνέχεια , το εμποδίζει να εκτελεστεί έως ότου επιλέξουμε να το επαναφέρουμε ή να το αφαιρέσουμε από τον υπολογιστή μας .

- **Αφαίρεση .** Διαγράφει μόνιμα το λογισμικό από τον υπολογιστή μας .

- **Να επιτρέπεται πάντα .** Προσθέτει το λογισμικό στην λίστα επιτρεπόμενων του Windows Defender και επιτρέπει την λειτουργία του στον υπολογιστή μας . Το Windows Defender θα σταματήσει να μας προειδοποιεί για τους κινδύνους που ίσως ενέχει το λογισμικό για τα προσωπικά μας δεδομένα ή τον υπολογιστή μας . Εδώ πρέπει να τονίσουμε ότι προσθέτουμε κάποιο λογισμικό στην λίστα επιτρεπόμενων του Windows Defender μόνο όταν εμπιστευόμαστε το λογισμικό αυτό και τον εκδότη του .

Το Windows Defender επίσης μας προειδοποιεί εάν κάποια προγράμματα επιχειρήσουν να αλλάξουν σημαντικές ρυθμίσεις των Windows . Επειδή το λογισμικό ήδη λειτουργεί στον υπολογιστή μας , μπορούμε να επιλέξουμε μια από τις παρακάτω ενέργειες :

- **Επιτρέπεται .** Επιτρέπεται το λογισμικό να αλλάζει τις ρυθμίσεις του υπολογιστή μας που σχετίζονται με την ασφάλεια .

- **Άρνηση**. Αποτρέπει το λογισμικό από το να αλλάζει τις ρυθμίσεις του υπολογιστή μας που7 σχετίζονται με την ασφάλεια .

Μπορούμε ακόμη να επιλέξουμε το λογισμικό και τις ρυθμίσεις που θέλουμε να παρακολουθεί το Windows Defender , αλλά οι κατασκευαστές μας συνιστάνε να χρησιμοποιούμε όλες τις ρυθμίσεις προστασίας σε πραγματικό χρόνο , που λέγονται **παράγοντες** . Ο παρακάτω πίνακας εξηγεί τον κάθε παράγοντα και γιατί είναι σημαντικός.

Πίνακας 1: Κατανόηση παραγόντων προστασίας σε πραγματικό χρόνο .

Κατανόηση παραγόντων προστασίας σε πραγματικό χρόνο .	
Παράγοντες προστασίας σε πραγματικό χρόνο	**Σκοπός**
Αυτόματη Εκκίνηση	Παρακολουθεί καταλόγους προγραμμάτων που επιτρέπεται να λειτουργούν αυτομάτως όταν εκκινείτε ο υπολογιστής μας .Το λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό μπορεί να ρυθμιστεί να λειτουργεί αυτόματα όταν εκκινούνται τα Windows . Έτσι μπορεί να λειτουργεί χωρίς να το γνωρίζουμε και να συλλέγει πληροφορίες , Μπορεί επίσης να κάνει τον υπολογιστή μας να εκκινεί ή να λειτουργεί αργά .
Διαμόρφωση συστήματος (Ρυθμίσεις)	Παρακολουθεί τις ρυθμίσεις που σχετίζονται με την ασφάλεια στα Windows . Το λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό μπορεί να αλλάζει τις ρυθμίσεις ασφάλειας του λογισμικό και του εξοπλισμού και , έπειτα , να συλλέγει πληροφορίες που μπορούν αν χρησιμοποιηθούν και να υπονομεύσουν περισσότερο την ασφάλεια του υπολογιστή μας .

Πρόσθετα του Internet Explorer	Παρακολουθεί προγράμματα που εκτελούνται αυτόματα όταν εκκινείτε ο Internet Explorer . Τα λογισμικά υποκλοπής spyware και άλλα πιθανώς ανεπιθύμητα λογισμικά μπορούν να μεταμφιεστούν ως πρόσθετα των προγραμμάτων περιήγησης του web και να εκτελούνται χωρίς να το γνωρίζουμε .
Διαμορφώσεις Internet Explorer (Ρυθμίσεις)	Εποπτεύει τις ρυθμίσεις ασφάλειας του προγράμματος περιήγησης , οι οποίες αποτελούν την πρώτη γραμμή άμυνας από το κακόβουλο περιεχόμενο στο Internet . Το λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό μπορεί να επιχειρήσει να αλλάξει τις ρυθμίσεις αυτές χωρίς να το γνωρίσουμε .
Αρχεία λήψης Internet Explorer	Εποπτεύει τα αρχεία και τα προγράμματα που έχουν σχεδιαστεί να λειτουργούν με το Internet Explorer , όπως τα στοιχεία ελέγχου ActiveX και τα προγράμματα εγκατάστασης λογισμικού . Αυτά τα αρχεία μπορούν να κάνουν αυτόματα λήψη , να εγκατασταθούν και να εκτελεστούν . Τα αρχεία αυτά μπορούν να περιλαμβάνουν και λογισμικό υποκλοπής spyware ή πιθανώς ανεπιθύμητο λογισμικό το οποίο θα εγκατασταθεί χωρίς να το γνωρίζουμε .
Υπηρεσίες και προγράμματα οδήγησης	Εποπτεύει τις υπηρεσίες και τα προγράμματα οδήγησης καθώς αλληλεπιδρούν με τα Windows και τα προγράμματα μας .Επειδή οι υπηρεσίες και τα προγράμματα οδήγησης εκτελούν απαραίτητες λειτουργίες του υπολογιστή μας (‘όπως το να επιτρέπουν στις συσκευές να συνεργάζονται με τον υπολογιστή μας) , έχουν πρόσβαση σε σημαντικό λογισμικό του λειτουργικού μας συστήματος . Το λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό μπορεί να χρησιμοποιεί τις υπηρεσίες και τα προγράμματα οδήγησης για να προσπελαύνει τον υπολογιστή μας ή να επιχειρεί να εκτελεστεί απαρατήρητο στον υπολογιστή μας , όπως τα κανονικά στοιχεία του λειτουργικού συστήματος .
Εκτέλεση εφαρμογής	Παρακολουθεί όταν τα προγράμματα εκκινούνται , καθώς και τις λειτουργίες που εκτελούν όταν εκτελούνται . Το λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό μπορεί να εκμεταλλεύεται τα τρωτά σημεία των προγραμμάτων που έχουμε εγκαταστήσει για την εκτέλεση κακόβουλου ή ανεπιθύμητου λογισμικού χωρίς να το γνωρίζουμε . Για

	παράδειγμα το λογισμικό υποκλοπής spyware μπορεί να εκτελείται αυτόματα στο παρασκήνιο όταν εκκινήσουμε κάποιο πρόγραμμα που χρησιμοποιούμε συχνά . Το Windows Defender παρακολουθεί τα προγράμματα μας και μας προειδοποιεί εάν ανιχνεύσει ύποπτη δραστηριότητα.
Δήλωση εφαρμογής	Παρακολουθεί τα εργαλεία και τα αρχεία στο λειτουργικό σύστημα, όπου μπορούν να εγγραφούν τα προγράμματα και να εκτελεστούν οποιαδήποτε στιγμή και όχι μόνο όταν εκκινούμε τα Windows ή κάποιο άλλο πρόγραμμα . Το λογισμικό Το λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό μπορεί να καταχωρίσει ένα πρόγραμμα για αν εκκινείτε χωρίς ειδοποίηση και να εκτελείται ,για παράδειγμα, μια προγραμματισμένη ώρα κάθε μέρα . Αυτό επιτρέπει στο πρόγραμμα να συλλέγει πληροφορίες σχετικά με εμάς ή τον υπολογιστή μας ή να κερδίσει πρόσβαση σε σημαντικό λογισμικό του λειτουργικού συστήματος , χωρίς να το γνωρίζουμε .
Πρόσθετα των Windows	Εποπτεύει τα πρόσθετα προγράμματα (γνωστά και ως βοηθητικά προγράμματα λογισμικού) των Windows . Τα πρόσθετα είναι σχεδιασμένα για να βελτιώνουν την εμπειρία μας με τον υπολογιστή σε τομείς όπως η ασφάλεια , η περιήγηση , η παραγωγικότητα και τα πολυμέσα .Ωστόσο τα πρόσθετα μπορούν επίσης να εγκαθιστούν προγράμματα που συλλέγουν πληροφορίες σχετικές με εμάς ή τις διαδικτυακές δραστηριότητες μας και να εκθέτουν ευαίσθητα , προσωπικά δεδομένα , πχ σε διαφημιστές .

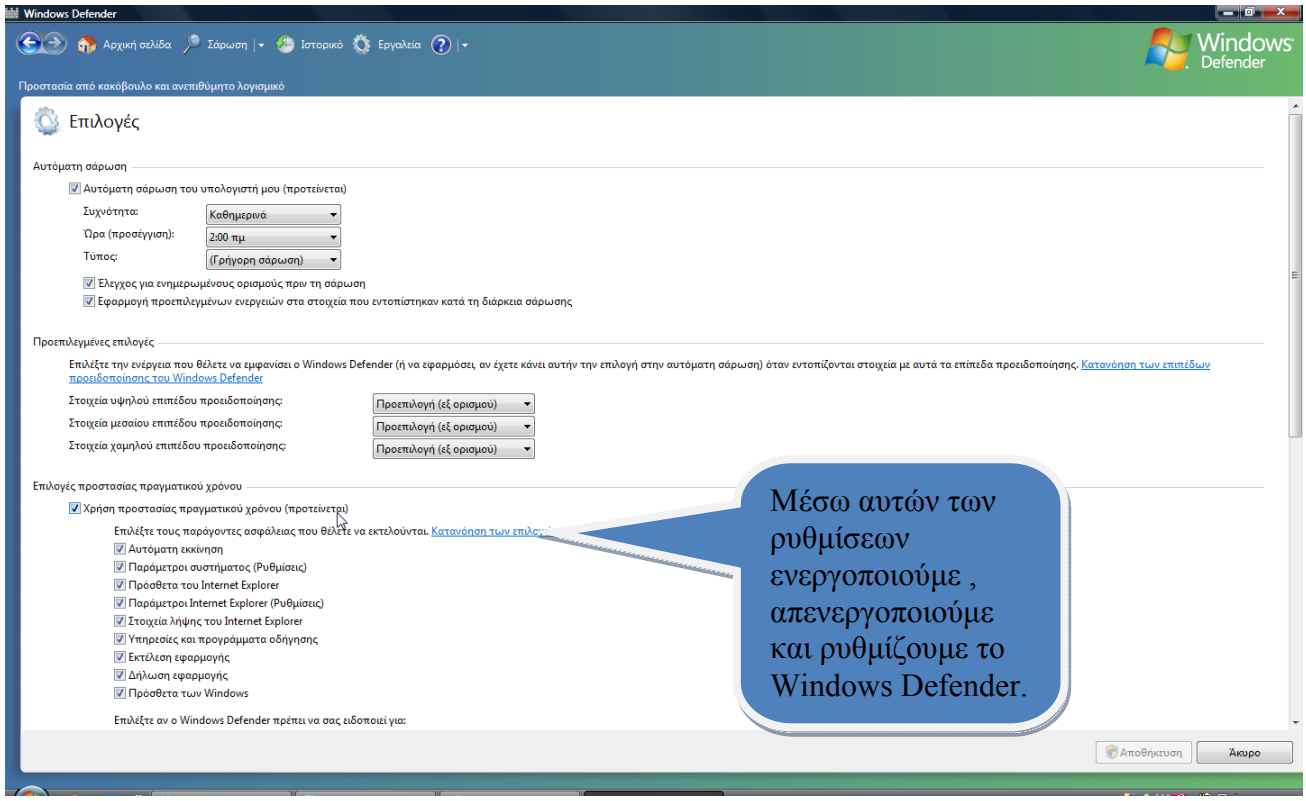
5.1.3.5.1 Ενεργοποίηση ή απενεργοποίηση της προστασίας σε πραγματικό χρόνο του Windows Defender.

Για τους λόγους που προαναφέραμε η προστασία σε πραγματικό χρόνο καθιστάται πολύ σημαντική . Στο σημείο αυτό θα αναφέρουμε τα βήματα και τις ενέργειες στις οποίες πρέπει να προβούμε προκειμένου να απενεργοποιήσουμε και να ενεργοποιήσουμε την προστασία σε πραγματικό χρόνο.

Για να εμποδίσουμε λογισμικό υποκλοπών ή άλλο ανεπιθύμητο λογισμικό να προσβάλλει τον υπολογιστή μας , ενεργοποιούμε την Προστασία σε πραγματικό χρόνο του Windows Defender και κάνουμε όλες τις επιλογές προστασίας σε πραγματικό χρόνο . Η προστασία σε πραγματικό χρόνο μας προειδοποιεί όταν κάποιο λογισμικό υποκλοπής spyware ή άλλο ανεπιθύμητο λογισμικό επιχειρήσει να εγκατασταθεί ή να εκτελεστεί στον υπολογιστή μας . Επίσης μας προειδοποιεί εάν κάποιο από τα προγράμματα επιχειρήσουν να αλλάξουν σημαντικές ρυθμίσεις των Windows .

Τα βήματα που ακολουθούμε για την επίτευξη της ενεργοποίησης ή απενεργοποίησης είναι τα ακόλουθα :

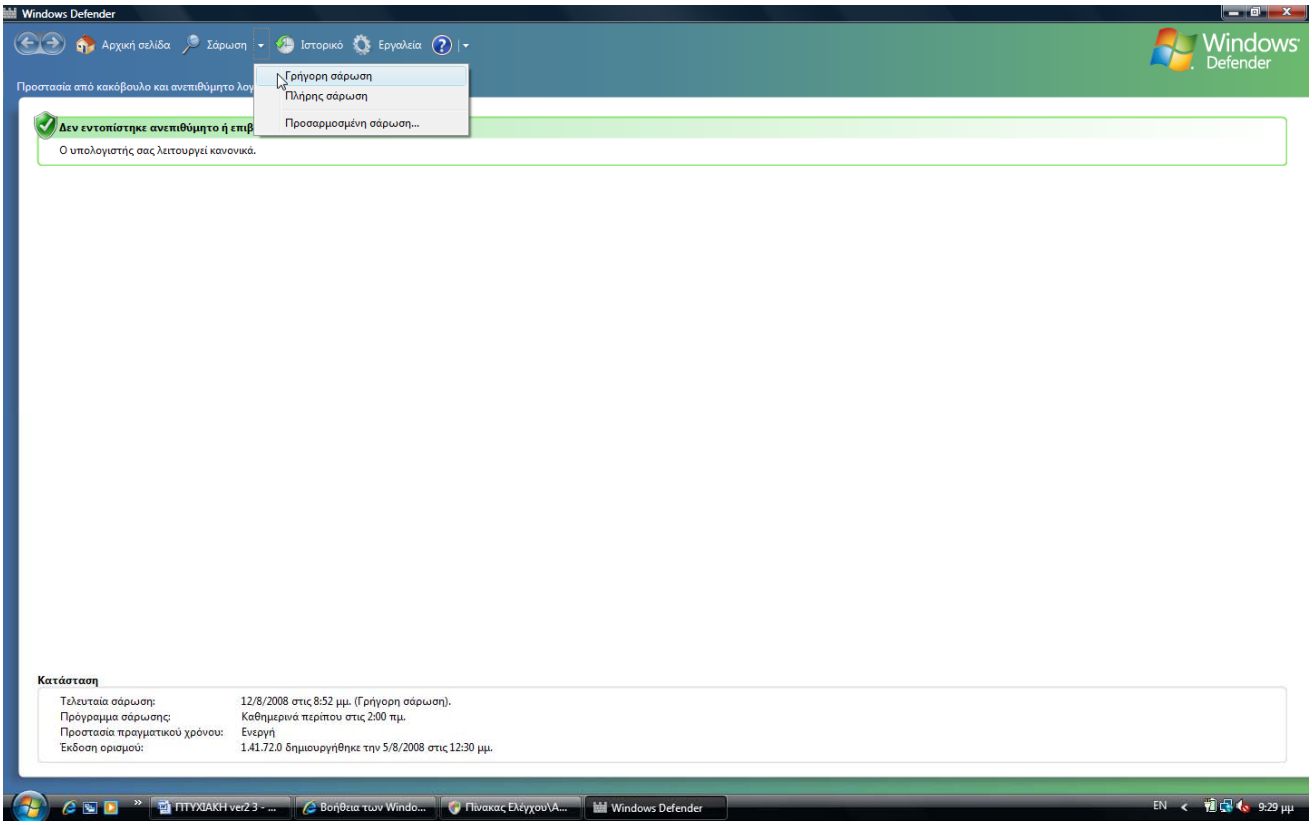
1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender** .
2. Κάνουμε κλικ στο μενού **Εργαλεία** και στην συνέχεια κάνουμε κλικ στην εντολή **Επιλογές**.
3. Στην επιλογή **Επιλογές προστασίας σε πραγματικό χρόνο** , επιλέγουμε το πλαίσιο ελέγχου **Χρήση προστασίας πραγματικού χρόνου (προτείνεται)**.
4. Ενεργοποιούμε τις επιλογές που θέλουμε . Για να προστατέψουμε τα προσωπικά μας δεδομένα και τον υπολογιστή μας , συνιστάται να επιλέξουμε όλες τις επιλογές προστασίας σε πραγματικό χρόνο .
5. Στην επιλογή **Επιλέξτε εάν θέλετε να σας ειδοποιεί ο Windows Defender σχετικά με τα παρακάτω :** , κάνουμε τις επιλογές που θέλουμε και έπειτα κάνουμε κλικ στο κουμπί **Αποθήκευση** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση .



Εικόνα 32: Παράθυρο Επιλογές του Windows Defender των Windows .

5.1.3.6 Έναρξη σάρωσης για λογισμικό υποκλοπής spyware ή άλλο πιθανώς ανεπιθύμητο λογισμικό .

Στο Windows Defender, μπορούμε να επιλέξουμε να εκτελέσουμε **γρήγορη σάρωση** του υπολογιστή μας ή **μια πλήρης σάρωση** του συστήματος . Εάν υποψιαζόμαστε ότι λογισμικό υποκλοπών έχει προσβάλει μια συγκεκριμένη περιοχή του υπολογιστή μας , μπορούμε να προσαρμόσουμε μια σάρωση επιλέγοντας μόνο τις μονάδες και τους φακέλους που θέλουμε να ελέγξουμε.



Εικόνα 33 : Παράθυρο Αρχική σελίδα του Windows Defender των Windows .

Κατά την γρήγορη σάρωση , ελέγχονται οι περιοχές στο σκληρό δίσκο του υπολογιστή μας τις οποίες είναι πιθανότερο να προσβάλει το λογισμικό υποκλοπών . Κατά την πλήρη σάρωση ελέγχονται όλα τα αρχεία στο σκληρό δίσκο του υπολογιστή μας και όλα τα προγράμματα που εκτελούνται εκείνη την στιγμή . Ωστόσο ,η ταχύτητα του υπολογιστή ενδέχεται να μειωθεί έως ότου να ολοκληρωθεί η σάρωση . Συνιστάται γενικά να προγραμματίζουμε μια καθημερινή γρήγορη σάρωση . Οποιαδήποτε στιγμή , εάν έχουμε υπόνοιες ότι λογισμικό υποκλοπών έχει προσβάλει τον υπολογιστή μας να εκτελούμε πλήρη σάρωση .

5.1.3.6.1 Γρήγορη σάρωση

Για να σαρώσουμε τις περιοχές του υπολογιστή μας τις οποίες είναι πιο πιθανόν να προσβάλλει το λογισμικό υποκλοπής spyware ακολουθούμε τα παρακάτω βήματα :

1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender** .
2. Κάνουμε κλικ στο **Σάρωση** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση .

5.1.3.6.2 Πλήρης σάρωση

Για να σαρώσουμε όλες τις περιοχές του υπολογιστή μας ακολουθούμε τα παρακάτω βήματα :

1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender** .

2. Κάνουμε κλικ στο **Βέλος προς τα κάτω** δίπλα στο κουμπί **Σάρωση** και μετά κάνουμε κλικ στην επιλογή **Πλήρης σάρωση** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση .

5.1.3.6.3 Προσαρμοσμένη σάρωση

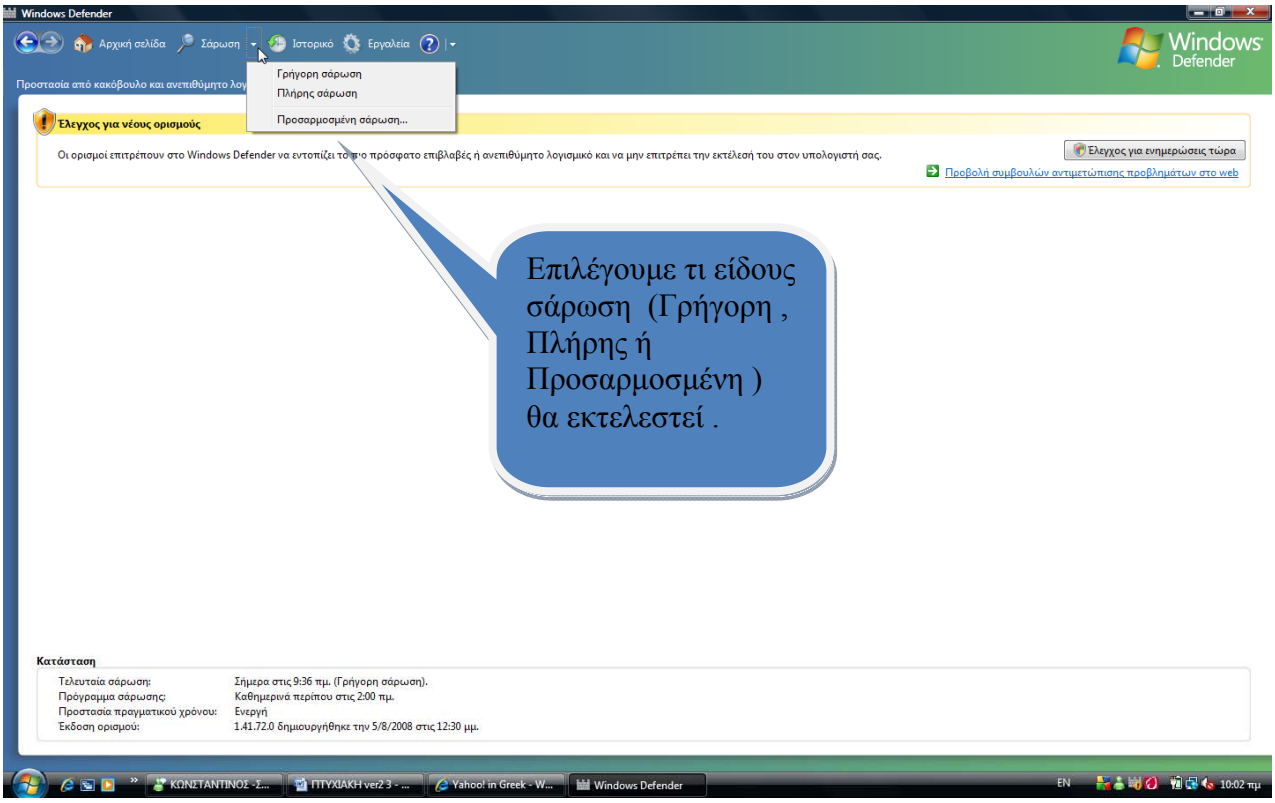
Μπορούμε να επιλέξουμε συγκεκριμένες επιλογές του υπολογιστή μας για να σαρωθούν από το Windows Defender. Ωστόσο εάν ανιχνευτεί πιθανώς ανεπιθύμητο ή κακόβουλο λογισμικό , το Windows Defender θα εκτελέσει γρήγορη σάρωση , έτσι ώστε τα στοιχεία που ανιχνεύτηκαν να αφαιρεθούν από τις άλλες περιοχές του υπολογιστή μας, εάν χρειαστεί .
Για να εφαρμόσουμε προσαρμοσμένη σάρωση του υπολογιστή μας ακολουθούμε τα παρακάτω βήματα :

1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender.**

2. Κάνουμε κλικ στο **Βέλος προς τα κάτω** δίπλα στο κουμπί **Σάρωση** και μετά κάνουμε κλικ στην επιλογή **Πλήρης σάρωση** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση .

3. Κάνουμε κλικ στην επιλογή **Σάρωση επιλεγμένων μονάδων δίσκου και φακέλων** και μετά κάνουμε κλικ στο **Επιλογή** .

4. Επιλέγουμε τις μονάδες δίσκου και τους φακέλους που θέλουμε να σαρώσουμε και κάνουμε κλικ στο κουμπί **OK** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση .



Εικόνα 34 : Παράθυρο Αρχική σελίδα του Windows Defender των Windows .

5.1.3.6.4 Επιλογή επιλογών σάρωσης για προχωρημένους

Όταν εκτελούμε σάρωση στον υπολογιστή μας μπορούμε να επιλέξουμε μια από τις παρακάτω επιπρόσθετες τέσσερις επιλογές :

- **Σάρωση των περιεχομένων των αρχειοθετημένων αρχείων και φακέλων για πιθανές απειλές .**
  Η σάρωση αυτών των σημείων ίσως αυξήσει τον χρόνο που απαιτείται για την ολοκλήρωση μιας σάρωσης , αλλά το λογισμικό υποκλοπής spyware και άλλο πιθανώς ανεπιθύμητο λογισμικό μπορεί να εγκατασταθεί αυτόματα και να επιχειρήσει να ¨κρυφτεί ¨σε αυτές τις θέσεις .

- **Χρήση ευρετικής μεθόδου για εντοπισμό πιθανώς επιβλαβούς ή ανεπιθύμητης συμπεριφοράς από λογισμικό που δεν έχει αναλυθεί για πιθανούς κινδύνους.**

  το Windows Defender χρησιμοποιεί αρχεία ορισμών για την αναγνώριση των γνωστών απειλών , αλλά μπορεί επίσης να ανιχνεύσει και να μας προειδοποιήσει για πιθανώς επιβλαβές ή ανεπιθύμητο λογισμικό που δεν έχει ακόμη καταγραφεί σε αρχείο ορισμού .

- **Δημιουργία σημείου επαναφοράς πριν την εφαρμογή ενεργειών στα εντοπισμένα στοιχεία.**
  Επειδή έχουμε την δυνατότητα να ορίσουμε το Windows Defender ώστε να καταγράφει αυτόματα τα εντοπισμένα στοιχεία , η επιλογή αυτή μας επιτρέπει να επαναφέρουμε τις ρυθμίσεις του συστήματος σε περίπτωση που θέλουμε να χρησιμοποιήσουμε λογισμικό που δεν σκοπεύαμε να καταργήσουμε .

- **Να μην γίνετε σάρωση στα παρακάτω αρχεία ή θέσεις .**
  Χρησιμοποιούμε αυτήν την τελευταία επιλογή για επιλογή αρχείων και φακέλων που δεν θέλουμε να σαρώσει το Windows Defender .

    1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender.**
    2. Κάνουμε κλικ στο μενού **Εργαλεία** και στην συνέχεια κάνουμε κλικ στην εντολή **Επιλογές.**
    3. Στην ενότητα **Επιλογές για προχωρημένους** , επιλέγουμε το πλαίσιο επιλογής που υπάρχει πλάι σε κάθε επιλογή που θέλουμε να χρησιμοποιήσουμε .
    4. Αν δεν θέλουμε το Windows Defender να σαρώσει ορισμένα σημεία του υπολογιστή μας , στο μενού επιλογών **Να μην γίνεται σάρωση στα παρακάτω αρχεία ή θέσεις ,** κάνουμε κλικ στην επιλογή **Προσθήκη** .
    5. Επιλέγουμε τα αρχεία ή τους φακέλους που δεν θέλουμε να σαρώσουμε και μετά επιλέγουμε **OK.** Επαναλαμβάνουμε το βήμα αυτό για κάθε αρχείο ή φάκελο που δεν θέλουμε να σαρώσουμε .
    6. Όταν ολοκληρώσουμε τις επιλογές για προχωρημένους , κάνουμε κλικ στο κουμπί **Αποθήκευση** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση.

5.1.3.7 Κατανόηση των επιπέδων προειδοποίησης του Windows Defender .

Η κατανόηση των επιπέδων προειδοποίησης είναι ένα σημαντικό ζήτημα , γιατί μας βοηθάει να επιλέξουμε με ποιον τρόπο θα αντιμετωπίσουμε το λογισμικό υποκλοπής και το πιθανώς ανεπιθύμητο λογισμικό . Σε κάποιες περιπτώσεις ο Windows Defender ίσως μας προτείνει να αφαιρέσουν το λογισμικό υποκλοπής spyware , δεν είναι όμως όλο το λογισμικό που ανιχνεύεται κακόβουλο ή ανεπιθύμητο . Οι πληροφορίες που παίρνουμε από τον ακόλουθο πίνακα μπορούν να μας βοηθήσουν να αποφασίσουμε τι θα πρέπει να κάνουμε εάν το Windows Defender ανιχνεύσει στον υπολογιστή μας κακόβουλο λογισμικό .

Πίνακας 2: Κατανόηση των επιπέδων προειδοποίησης του Windows Defender.

Κατανόηση των επιπέδων προειδοποίησης του Windows Defender		
Επίπεδο Προειδοποίησης	**Τι σημαίνει ;**	**Τι πρέπει να κάνουμε ;**
Σοβαρή	Ευρέως διαδεδομένα ή ιδιαίτερα κακόβουλα προγράμματα , όπως οι ιοί ή ιοί τύπου worm, τα οποία απειλούν τα προσωπικά μας δεδομένα και την ασφάλεια του υπολογιστή μας και μπορούν να προκαλέσουν βλάβη σε αυτόν	Να αφαιρέσουμε το λογισμικό αυτό αμέσως .
Υψηλή	Προγράμματα που μπορεί να συλλέγουν τα προσωπικά μας δεδομένα και να απειλούν το απόρρητο μας ή να προκαλούν βλάβες στον υπολογιστή μας , για παράδειγμα συλλέγοντας πληροφορίες ή αλλάζοντας τις ρυθμίσεις , συνήθως χωρίς να το γνωρίζουμε και χωρίς την συγκατάθεσή μας .	Να αφαιρέσουμε το λογισμικό αυτό αμέσως .
Μεσαία	Προγράμματα που πιθανόν να επηρεάσουν το απόρρητο των προσωπικών μας δεδομένων ή να κάνουν αλλαγές στον υπολογιστή μας οι οποίες θα μπορούσαν να επηρεάσουν αρνητικά την απόδοσή του , για παράδειγμα συλλέγοντας προσωπικές πληροφορίες ή αλλάζοντας ρυθμίσει ς	Πρέπει να δούμε τις λεπτομέρειες της προειδοποίησης για να δούμε για ποίο λόγο ανιχνεύτηκε το λογισμικό . Εάν δεν μας αρέσει ο τρόπος με τον οποίο λειτουργεί το λογισμικό ή εάν δεν αναγνωρίζουμε ή δεν εμπιστευόμαστε τον εκδότη , θα πρέπει να εμποδίσουμε ή να καταργήσουμε το λογισμικό.
Χαμηλή	Πιθανώς ανεπιθύμητο λογισμικό που ίσως συλλέγει πληροφορίες σχετικά με εμάς ή τον υπολογιστή μας ή αλλάζει τον τρόπο με τον οποίο λειτουργεί ο υπολογιστής μας , αλλά λειτουργεί σύμφωνα με τους όρους	Αυτό το λογισμικό συνήθως δεν είναι επιβλαβές όταν λειτουργεί στον υπολογιστή μας , εκτός εάν έχει εγκατασταθεί χωρίς να το γνωρίζουμε. Αν δεν είμαστε βέβαιοι αν θέλουμε ν α το

	της άδειας χρήσης που εμφανίζονται όταν εγκαθιστάται το λογισμικό .	επιτρέψουμε , πρέπει να δούμε τις λεπτομέρειες της προειδοποίησης ή να δούμε αν αναγνωρίζουμε και εμπιστευόμαστε τον εκδότη του λογισμικού.
Δεν έχει ταξινομηθεί ακόμη	Προγράμματα που συνήθως δεν είναι επιβλαβή εκτός εάν έχουν εγκατασταθεί στον υπολογιστή μας χωρίς να το γνωρίζουμε .	Αν αναγνωρίζουμε και εμπιστευόμαστε το λογισμικό επιτρέπουμε την λειτουργία του. Αν δεν αναγνωρίζουμε το λογισμικό ή τον εκδότη , πρέπει να δούμε τις λεπτομέρειες της ειδοποίησης και αποφασίζουμε πως θα ενεργήσουμε . Αν δεν συμμετέχουμε στην κοινότητα Spy Net , μπορούμε να δούμε τις ταξινομήσεις της κοινότητας για να δούμε αν οι άλλοι χρήστες εμπιστεύονται το λογισμικό .

5.1.3.8 Προγραμματίζουμε πότε ο Windows Defender θα εκτελεί σάρωση του υπολογιστή μας .

Όπως και με τις ρυθμίσεις για προχωρημένους που προαναφέραμε έτσι και σε αυτό το κομμάτι οι δημιουργοί συνιστούν να προγραμματίζουμε μια καθημερινή γρήγορη σάρωση . Η γρήγορη σάρωση θα ελέγξει τις περιοχές του υπολογιστή μας τις οποίες είναι πιθανότερο να προσβάλλει λογισμικό υποκλοπής spyware και άλλο ανεπιθύμητο λογισμικό . Στην συνέχεια να θέλουμε να ελεγχτούν όλα τα αρχεία και τα προγράμματα μας στον υπολογιστή , εκτελούμε ή προγραμματίζουμε μια πλήρης σάρωση .

Ακόμη για να ενισχύσουμε την ασφάλεια του υπολογιστή μας , μπορούμε να επιλέξουμε να καταργείται αυτόματα το λογισμικό υποκλοπής spyware ή άλλο ανεπιθύμητο λογισμικό που θα ανιχνευτεί κατά την διάρκεια της σάρωσης.

Τα βήματα που ακολουθάμε για να προγραμματίσουμε τις σαρώσεις του Windows Defender είναι τα ακόλουθα :

1. Ανοίγουμε το Windows Defender κάνοντας κλικ στο κουμπί **Έναρξη** , έπειτα κάνουμε κλικ στην επιλογή **Όλα τα προγράμματα,** και στην συνέχεια επιλέγουμε **Windows Defender.**

2. Κάνουμε κλικ στο μενού **Εργαλεία** και στην συνέχεια κάνουμε κλικ στην εντολή **Επιλογές**.

3. Στην επιλογή **Αυτόματη σάρωση** επιλέγουμε το πλαίσιο επιλογής **Αυτόματη σάρωση του υπολογιστή μου (προτείνεται)** και μετά επιλέγουμε την συχνότητα , την ημέρα ,και τον τύπο σάρωσης που θέλουμε να εκτελείται .

4. Για να αφαιρείται αυτόματα το λογισμικό υποκλοπής ή άλλο πιθανώς ανεπιθύμητο λογισμικό μετά από την σάρωση , επιλέγουμε το πλαίσιο **Εφαρμογή προεπιλεγμένων ενεργειών σε στοιχεία που εντοπίστηκαν κατά την σάρωση .**

5. Στην επιλογή **Προεπιλεγμένες ενέργειες ,** επιλέγουμε την ενέργεια που θέλουμε να εκτελείται σε κάθε προειδοποίηση του Windows Defender και κάνουμε κλικ στο κουμπί **Αποθήκευση** . Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή παρέχουμε την επιβεβαίωση.

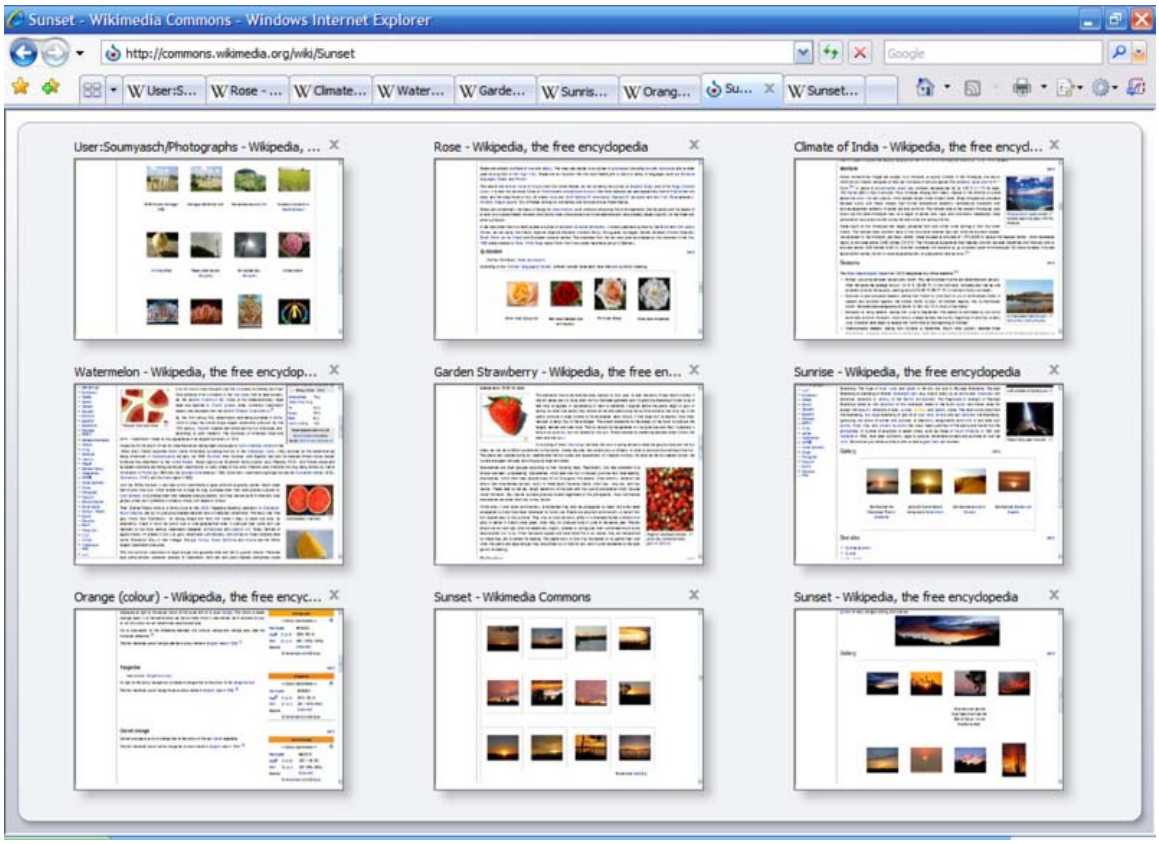
6 ΝΕΟΣ ΒΕΛΤΙΩΜΕΝΟΣ INTERNET EXPLORER 7

Ο παλιότερα γνωστός Microsoft Internet Explorer , με συντομογραφία MSIE , με την κοινή συντομογραφία IE , είναι ένα πρόγραμμα πλοήγησης σελίδων (browser) για το διαδίκτυο της εταιρίας Microsoft και περιλαμβάνεται πλέον ως μέρος των λειτουργικών συστημάτων Microsoft . Η νέα και βελτιωμένη έκδοση του Windows Internet Explorer , η version 7 είναι πλέον γεγονός . Η έκδοση 7 μετονομάστηκε σε Windows Internet Explorer , ως κομμάτι των νέων χαρακτηριστικών ασφάλειας της Microsoft που περιλαμβάνονται στα Windows . Είναι ένα διαδεδομένο πρόγραμμα περιήγησης ιστοσελίδων .Αποτελεί και αυτό ενσωματωμένο τμήμα των λειτουργικών συστημάτων της Microsoft . Ο IE προσφέρει συμβατότητα σχεδόν με όλες τις ιστοσελίδες που ακολουθούν το πρότυπο HTML, αλλά και με πολλές άλλες που είναι σχεδιασμένες ειδικά για αυτόν.

Κυκλοφόρησε στις αρχές του 2007 και είναι συμβατός τόσο στα Windows Vista όσο και στις προηγούμενες εκδόσεις αυτών δηλαδή τα Windows XP SP2 και Windows Server 2003 SP1.
Ο Internet Explorer 7 είναι ένα κομμάτι μιας μεγάλης γραμμής εκδόσεων των Internet Explorer , και η πρώτη σημαντική έκδοσης μιας μηχανής αναζήτησης για πάνω από 5 έτη . Στέλνει πληροφορίες ως εξορισμού browser στα Windows Vista και αποτελεί την εξελιγμένη έκδοση του Internet Explorer 6 των Windows XP .
Ένα από τα νέα χαρακτηριστικά γνωρίσματα του νέου αυτού λειτουργικού συστήματος είναι η προηγμένη και ασφαλής περιήγηση που παρέχει .

Είναι διαθέσιμος όπως προαναφέραμε ως κομμάτι των Windows Vista ,των Windows Server 2008 , και μπορεί να το κατεβάσουμε ως ξεχωριστό πρόγραμμα μέσω του Windows Update ξεκινώντας από τις εκδόσεις Windows XP με Sp 2 και Windows Server 2003 με SP1 και SP2 . Τον Windows Internet Explorer μπορούμε ακόμη να τον προμηθευτούμε απευθείας από το website της Microsoft . Ένα μεγάλο μέρος της παλιάς αρχιτεκτονικής , συμπεριλαμβανομένης της μηχανής απόδοσης και του πλαισίου ασφάλειας έχουν συμπεριληφθεί στο νέο Windows Internet Explorer. Εν μέρει σαν αποτέλεσμα των αυξήσεων ασφάλειας , ο νέος αυτός browser είναι μια αυτόνομη εφαρμογή , και όχι ενσωματωμένος με τα υπόλοιπα παράθυρα και δεν είναι έτσι πλέον σε θέση να λειτουργεί ως μηχανή αναζήτησης αρχείων .

Ο IE 7 έχει ανανεωμένη επιφάνεια εργασίας . Μπορεί να ανοίξει ιστοσελίδες σε διαφορετικές καρτέλες του ίδιου παραθύρου , όπως ήδη συμβαίνει στον Firefox, στον Netscape και στον Opera , ενώ περιλαμβάνει και την λειτουργία ¨ **Γρήγορες καρτέλες** ¨ **(Quick tabs)**, με την οποία εμφανίζονται τα περιεχόμενα των καρτελών που έχουμε επισκεφτεί σαν μικρογραφίες και μπορούμε να ανακατευθυνθούμε σε αυτές , επιλέγοντας κάποια από τις μικρογραφίες .



Εικόνα 35: Παράθυρο εμφάνισης των Quick Tabs του Internet Explorer 7.

Στα Windows Vista , ο Internet Explorer λειτουργεί με έναν νέο ¨Προστατευτικό τρόπο ¨ , ο οποίος τρέχει τον browser σε ένα ασφαλές sandbox και το οποίο δεν έχει πρόσβαση στο υπόλοιπο λειτουργικό σύστημα ή στα αρχεία του συστήματος εκτός από τον φάκελο¨ Temporary Internet Files ¨ .
Όταν λειτουργεί σε **Προστατευμένη λειτουργία** ο Internet Explorer 7, χαρακτηρίζεται ως χαμηλής ακεραιότητας διαδικασία , γεγονός που έχει σαν αποτέλεσμα ότι δεν μπορεί να παρέχει γραπτή πρόσβαση σε αρχεία και σε κλειδιά τις registry τα οποία βρίσκονται έξω από τον φάκελο του προφίλ του χρήστη.
Αυτό το χαρακτηριστικό γνώρισμα στοχεύει να μετριάσει τα προβλήματα τα οποία είχαν να κάνουν με ρωγμές που έχουν πρόσφατα ανακαλυφθεί στον browser (ή σε πρόσθετες λειτουργίες που φιλοξενούσε μέσα του ο IE7 και οι οποίες διευκόλυναν τον εκάστοτε χάκερ να εγκαθιστά κακόβουλο λογισμικό στον υπολογιστή του χρήστη).
Ακόμη στην έκδοση 7 υποστηρίζεται και η **υπηρεσία RSS(Rich Site Summary)** , με την οποίαν μπορούν οι χρήστες να λαμβάνουν στο πρόγραμμα πλοήγησης τους , τίτλους ειδήσεων με τη χρήση της γλώσσας XML , από ιστοσελίδες που είναι συνδρομητές .

Όπως και στον Firefox , ο IE έχει τις δικές του **επεκτάσεις (add-ons)**.

Και τέλος ένα νέο και σημαντικό χαρακτηριστικό της έκδοσης 7 είναι η δυνατότητα προειδοποίησης για ύποπτες ιστοσελίδες , που παραποιούν στοιχεία τους ώστε να εμφανίζονται σαν ιστοσελίδες εταιρειών του οικονομικού τομέα κτλ (**Phishing**) .

Οι εκδόσεις του IE7 των Windows Vista και Windows XP , περιέχουν έναν επιπλέον χαρακτηριστικό γνώρισμα, **μια αναβάθμιση του Winlnet API** . Η νέα αυτή έκδοση διαθέτει **καλύτερη υποστήριξη του πρωτοκόλλου IPv6** , καθώς επίσης συμπεριλαμβάνει και **δεκαεξαδικά literals στις διευθύνσεις του IPv6** .
Τέλος συμπεριλαμβάνει καλύτερη υποστήριξη για την **Gzip και deflate συμπίεση** , έτσι ώστε η επικοινωνία με έναν κεντρικό υπολογιστή δικτύου να μπορεί να συμπιεστεί και έτσι να απαιτεί τα λιγότερα δυνατά στοιχεία για να μεταφερθούν .

Η προστατευμένη λειτουργία του Internet Explorer συμπεριλαμβάνεται και υποστηρίζεται αποκλειστικά στα Windows Vista . Ακόμη τον Οκτώβριο του 2007 , η Microsoft απέκοψε το συστατικό ασφάλειας **Windows Genuine Advantage** από τον IE7 , κάνοντάς το προσιτό σε όλους τους χρήστες των Windows.

Η έκδοση IE7 υποστηρίζει ακόμη τα **Internationalized domain names(IDN)** τα οποία συμπεριλαμβάνουν **anti-spoofing protection** . Για παράδειγμα εάν κάποιος χρήστης επισκεφτεί κάποιο site του οποίου το όνομα βρίσκεται σε μια ξένη γλώσσα (χωρίς λατινικούς χαρακτήρες), θα εμφανιστεί σε **Panycode** (ο panycode είναι προγραμματιστική κωδικοποιημένη σύνταξη στον υπολογιστή , στην οποία οι Unicode string χαρακτήρες μεταφράζονται στο σύνολο των αντίστοιχων περιορισμένων χαρακτήρων που είναι επιτρεπτοί για network host name).

Ένα **πλαίσιο αναζήτησης(search box)** έχει προστεθεί στην μπάρα εργαλείων του Internet Explorer . Η εξ ορισμού μηχανή αναζήτησης έχει κληρονομηθεί από την προηγούμενη έκδοση του , και η οποία διασυνδέεται με τις διάσημες μηχανές αναζήτησης όπως πχ Google, AltaVista,Yahoo, Live Search,Wikipedia .

Η **μπάρα διεύθυνσης καθώς και η μπάρα κατάστασης** εμφανίζεται σε όλα τα παράθυρα καθώς και στα αναδυόμενα , με τον τρόπο αυτό βοηθούνται οι χρήστες να καταλάβουν και να αποτρέψουν κακόβουλα site που είναι μεταμφιεσμένα ως αξιόπιστα.

Τα **modal windows** όπως τα dialog boxes εμφανίζονται μόνο όταν επιλέγεται η εκάστοτε ετικέτα του παραθύρου (στην περίπτωση αυτή η ετικέτα έχει χρώμα πορτοκαλί), και εκτός του γεγονός ότι είναι ασφαλή τα modal windows παρουσιάζονται με τέτοιο τρόπο ώστε ο χρήστης δεν μπορεί να κοιτάξει πάνω από ένα παράθυρο την φορά .

Η μπάρα κατάστασης δεν επιτρέπει πλέον σε συνηθισμένο κείμενο να εισάγεται και σε αντίθεση εμφανίζει πάντα την URL οποιασδήποτε σύνδεσης και αν επιδιώξουμε να κάνουμε . Εμφανίζεται επίσης και ο στόχος URL των form button, με αυτόν τον τρόπο μας βοηθάει να προσδιορίσουμε τις μορφές που υποβάλλουν τα στοιχεία τους στις ύποπτες περιοχές .

Η επιλογή **¨ Διαγραφή Ιστορικού Περιήγησης (Delete Browsing History) ¨** καθαρίζει εντελώς το ιστορικό περιήγησης με ένα απλό βήμα . Αρχικά αυτή ήταν μια πολυσύνθετη και πολυδιάστατη εργασία , απαιτούσε να διαγράψουμε αρχικά τα προσωρινά αρχεία Internet ,μετά τα cookies στην συνέχεια το ιστορικό ,τα δεδομένα φορμών και τέλος τους κωδικούς πρόσβασης και όλα αυτά πραγματοποιώντουσαν σε μια σειρά από βήματα . Αυτό το χαρακτηριστικό είναι πολύ χρήσιμο γιατί διασφαλίζει την μυστικότητα και την ασφάλεια μας ιδιαίτερα σε περιπτώσεις περιβάλλοντος πολλών χρηστών , όπως σε ένα Internet cafeé.

Η λειτουργία ¨**Fix My Settings**¨ ελέγχει τις ρυθμίσεις μας στην έναρξη ή όποτε άλλοτε αλλάζει μια ρύθμιση , και η νέα αυτή ρύθμιση δεν είναι ασφαλής ειδοποιεί τον χρήστη. Υπάρχει ακόμη η δυνατότητα ο χρήστης με το πάτημα ενός κουμπιού να ρυθμίσει όλες τις ιδιότητες του Internet Explorer και να τις θέσει σε ασφαλή πλαίσια .

Παλιά πρωτόκολλά και τεχνολογίες έχουν αφαιρεθεί : **Gopher**, **TELNET**, **Scriptlets** , **DirectAnimation**, **XBM** , **Channels** γνωστό ως **Active Desktop items** . Τέλος από τον Internet Explorer 7 των Windows Vista έχει αφαιρεθεί ακόμη το στοιχείο **DHTML Editor control** προκειμένου να μειωθούν οι επιθέσεις ασφάλειας της επιφάνειας εργασίας .

Δεν επιτρέπετε η χρησιμοποίηση των πρόσθετων εφαρμογών (Add-ons), εάν προηγουμένως δεν έχει επιτραπεί και ολοκληρωθεί η εγκατάστασή τους .

Του IE7 το **cipher-μήκος** είναι 256bit , αυτό ισχύει μόνο για τον IE7 στα Windows Vista γιατί ο IE7 στα Windows XP διαθέτει cipher-μήκος 128bit.
Η μπάρα διεύθυνσης μετατρέπεται σε κόκκινη όταν το πιστοποιητικό του site παρουσιάζει πρόβλημα ασφάλειας . Σε αυτήν την περίπτωση η περιήγηση στην περιοχή αυτή εμποδίζεται εξ ορισμού , και μπορεί μόνο να προσεγγιστεί και να επιτραπεί η περιήγηση σε αυτό , μόνο αφού την επιβεβαιώσει ρητά ο χρήστης .

Ο IE7 παρέχει ακόμη υποστήριξη για τα **Extended Validation Certificates (EV)** . Όταν ένα site διαθέτει και παρουσιάσει κάποιο EV , η μπάρα διεύθυνσης αλλάζει σε πράσινο χρώμα .

Νέα **Group Policy`s Administrative Templates** για τον IE7 φορτώνονται αυτόματα στον Domain controller , όταν μια Group Policy ανοίξει από κάποιον οργανισμό . Αυτά τα νέα διοικητικά πρότυπα επιτρέπουν τον έλεγχο του anti-phishing επιπέδου για παράδειγμα .

Reset Internet Explorer Settings, διαγράφει όλα τα προσωρινά αρχεία, απενεργοποιεί τα add-ons του browser και επαναφέρει στην αρχική κατάσταση όλες τις ρυθμίσεις που έχουν γίνει μέχρι την στιγμή εκείνη. Είναι μια χρήσιμη επιλογή σε περίπτωση που ο browser μας είναι σε μια κατάσταση ασυνήθιστη .

6.1 Εκδόσεις του Windows Internet Explorer

Τον Φεβρουάριο του 2005 ο Bill Gates μέσω της Microsoft ανακοίνωσε την κυκλοφορία του νέου web browser στο συνέδριο του San Francisco . Ο Internet Explorer 7 ήταν διαθέσιμος μόνο στα Windows XP με SP2 καθώς και σε μεταγενέστερες εκδόσεις των Windows συμπεριλαμβανομένων των Windows Server 2003 με SP1 και των Windows Vista .

Η πρώτη BETA έκδοση του νέου αυτού web browser κυκλοφόρησε τον Ιούλιο του 2007, κυκλοφόρησε κυρίως για τεχνική μελέτη . Η πρώτη δημόσια παρουσίαση στο κοινό της δεύτερης BETA έκδοσης έγινε τον Ιανουάριο του 2006 . Η τελική έκδοση κυκλοφόρησε τον Οκτώβριο του 2006. Την ίδια χρονική περίοδο το Yahoo παρείχε μια μετά-BETA έκδοση του Internet Explorer συσσωρευμένου με το Yahoo (όπως πχ εργαλειοθήκη και άλλες συγκεκριμένες προσαρμογές).

Η έκδοση 7 έχει ως πρωτεύοντα σκοπό να υπερασπίσει τους χρήστες από το **phishing** ή ακόμη από άλλο παραπλανητικό ή κακόβουλο λογισμικό, και χαρακτηρίζει επίσης τον **πλήρη έλεγχο χρηστών ActiveX** και του καλύτερου πλαισίου ασφάλειας το οποίο δεν φιλοξενείται στην διαδικασία του Windows Explorer, αλλά τρέχει αυτόνομα σε μια δική του διαδικασία.
Περιλαμβάνει ακόμη **bug fixes**, βελτιώσεις για την υποστήριξη των προτύπων του web, ακόμη διαθέτει όπως και προαναφέραμε την υπηρεσία **Γρήγορων καρτελών** , για πιο γρήγορη και

εύκολη διαχείριση των ιστοσελίδων , διαθέτει ένα **πολυμηχανικό πλαίσιο αναζήτησης** , **έναν web feeds reader** , υποστηρίζει διεθνοποιημένα domain names (IDN-Internationalized Domain Name) .

Για αυτά τα χαρακτηριστικά θα αναφερθούμε εκτενέστερα σε ακόλουθες παραγράφους .

6.2 Χαρακτηριστικά ασφαλείας του Microsoft Internet Explorer .

Η Microsoft αντιμετωπίζει τα προβλήματα ασφαλείας , που της προκύπτουν, με δύο κυρίως τρόπους , οι οποίοι κυρίως εμφανίζονται σε λογισμικά όπως τα Microsoft Vista.

- **Με χρήση του User Account Control** : ο οποίος αναγκάζει τον χρήστη να επιβεβαιώσει κάθε ενέργεια η οποία ενδέχεται να έχει επιπτώσεις σταθερότητας του συστήματος μας ή την ασφάλεια του συστήματος μας κάθε φορά που κάποιος χρήστη εισέρχεται στο σύστημα ως διαχειριστής.

- **Με την χρήση της προστατευμένης λειτουργίας** : η οποία τρέχει την διαδικασία του web server με πολύ λιγότερα προνόμια από ότι ο χρήστης .

6.2.1 Phishing filter

Στην γλώσσα των υπολογιστών , με την λέξη phishing εννοούμε την ποινικά ψευδή διαδικασία της προσπάθειας να αποκτηθούν , οι ευαίσθητες πληροφορίες όπως ονόματα χρήστη (username), κωδικοί (password) ,λεπτομέρειες και πληροφορίες πιστωτικών καρτών κα μέσω της μεταμφίεσης ως αξιόπιστης οντότητας σε μια ηλεκτρονική επικοινωνία.

Υπάρχουν επικοινωνίες οι οποίες ισχυρίζονται ότι είναι από οργανισμούς και εταιρείες όπως PayPal, eBay, YouTube, ή ηλεκτρονικές συναλλαγές τραπεζών και χρησιμοποιούνται κυρίως για να δελεάσουν ανυποψίαστους χρήστες .
Το Phishing πραγματοποιείται κυρίως μέσω ηλεκτρονικών μηνυμάτων (e-mail), ή άμεσων μηνυμάτων επικοινωνίας (instant messaging), και κατευθύνει με τέτοιο τρόπο τους χρήστες έτσι ώστε να εισάγουν λεπτομέρειες των προσωπικών τους στοιχείων στα web sites . Το Phishing είναι ένα παράδειγμα κοινωνικής τεχνικής εφαρμοσμένης μηχανικής που χρησιμοποιείται κυρίως για τους αφελής και μη έμπειρους χρήστες .

Γίνονται προσπάθειες για να εξεταστεί ο αυξανόμενος αριθμός του φαινομένου phishing . Μια από τις πρώτες τεχνικές phishing που περιγράφτηκε με λεπτομέρειες ήταν το 1987, και η πρώτη καταγεγραμμένη χρήση του όρου phishing έγινε το 1996. Ο όρος phishing είναι μια παραλλαγή του όρου της αλιείας , είναι πιθανώς επηρεασμένος από το όρο **phreaking** και υπαινίσσεται τα δολώματα που χρησιμοποιούνται για να ¨ψαρέψουν¨ οικονομικές πληροφορίες και κωδικούς.

Όπως προαναφέρθηκε το phishing στοχεύει στους πελάτες των τραπεζών και ιδιαίτερα αυτών που κάνουν συναλλαγές μέσω απευθείας σύνδεσης υπηρεσιών πληρωμής . Παράδειγμα αυτών , ηλεκτρονικά μηνύματα ,τα οποία στέλνονταν υποθετικά από υπηρεσίες εσωτερικού εισοδήματος , είχαν χρησιμοποιηθεί για να σταχυολογήσουν ευαίσθητα δεδομένα φορολογούμενων των ΗΠΑ. Και ενώ τα πρώτα μηνύματα αυτού του είδους είχα σταλθεί αδιακρίτως σε χρήστες , με το πέρασμα του χρόνου , έρευνες έδειξαν ότι τα phishers μπορούν σε γενικές γραμμές να καθορίσουν ποια θα είναι τα πιθανά τους θύματα , γεγονός που τα κάνει ακόμη πιο επικίνδυνα .

6.2.1.1 Τι είναι το Ηλεκτρονικό ¨ψάρεμα¨;

Το ηλεκτρονικό ¨ψάρεμα¨(στα Αγγλικά ¨phishing¨ από την λέξη fishing (ψάρεμα)),είναι ένας τρόπος παραπλάνησης των χρηστών υπολογιστών , με στόχο να πειστούν να αποκαλύψουν προσωπικές πληροφορίες ή οικονομικά στοιχεία , μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου ή τοποθεσίας web . Μια συνηθισμένη απάτη ηλεκτρονικού ¨ψαρέματος ¨ ξεκινά με ένα μήνυμα ηλεκτρονικού ταχυδρομείου το οποίο μοιάζει με μια επίσημη ειδοποίηση από μια αξιόπιστη πηγή , όπως μια τράπεζα, εταιρεία πιστωτικών καρτών ,ή ευυπόληπτη εταιρεία ηλεκτρονικού εμπορίου . Οι παραλήπτες του μηνύματος αυτού κατευθύνονται στο να επισκεφθούν μια τοποθεσία Web η οποία έχει δημιουργηθεί με στόχο την εξαπάτησή τους, , όπου τους ζητείται να παράσχουν προσωπικές πληροφορίες , όπως ο αριθμός ή ο κωδικός πρόσβασης κάποιου λογαριασμού τους .Στην συνέχεια , οι πληροφορίες αυτές χρησιμοποιούνται συνήθως για την υποκλοπή ταυτότητας .

6.2.1.2 Τι είναι το φίλτρο ηλεκτρονικού ¨ψαρέματος ¨ και πως συμβάλλει αυτό στην προστασία μου .

Το φίλτρο ηλεκτρονικού ¨ψαρέματος¨ της Microsoft είναι μια δυνατότητα του Internet Explorer η οποία συμβάλλει στον εντοπισμό τοποθεσιών του Web που έχουν σαν στόχο το ηλεκτρονικό ¨ψάρεμα¨ . Το φίλτρο ηλεκτρονικού ¨ψαρέματος¨ εκτελείται στο παρασκήνιο ενώ περιηγούμαστε στο Web και χρησιμοποιεί τρείς μεθόδους για την προστασία μας από τις απάτες ηλεκτρονικού ¨ψαρέματος¨ . Πρώτον , συγκρίνει τις διευθύνσεις των τοποθεσιών Web τις οποίες επισκεπτόμαστε με μια λίστα τοποθεσιών οι οποίες έχουν αναφερθεί στην Microsoft ως νόμιμες .Αυτή η λίστα είναι αποθηκευμένη στον υπολογιστή μας .Δεύτερος , συμβάλλει στην ανάλυση των τοποθεσιών τις οποίες επισκεπτόμαστε για να διαπιστωθεί εάν έχουν χαρακτηριστικά τα οποία είναι κοινά για τοποθεσίες Web που έχουν ως στόχο το ηλεκτρονικό ¨ψάρεμα¨ . Τρίτον με την συγκατάθεσή μας , το φίλτρο ηλεκτρονικού ¨ψαρέματος ¨, αποστέλλει ορισμένες διευθύνσεις Web στην Microsoft για περαιτέρω έλεγχο έναντι μιας λίστας τοποθεσιών Web ηλεκτρονικού ¨ψαρέματος ¨ που έχουν αναφερθεί και η οποία ενημερώνεται συχνά .

Εάν η τοποθεσία την οποία επισκεπτόμαστε συμπεριλαμβάνεται στην λίστα με τις τοποθεσίες Web ηλεκτρονικού ¨ψαρέματος ¨ , οι οποίες έχουν αναφερθεί ο Internet Explorer εμφανίζει μια ιστοσελίδα προειδοποίησης και μια ειδοποίηση στην γραμμή διευθύνσεων . Από την ιστοσελίδα προειδοποίησης μπορούμε να επιλέξουμε να συνεχίσουμε ή να κλείσουμε την σελίδα . Εάν η ιστοσελίδα περιέχει χαρακτηριστικά τα οποία είναι κοινά για τοποθεσίες Web ηλεκτρονικού ¨ψαρέματος ¨ , αλλά αυτή δεν συμπεριλαμβάνεται στην λίστα , ο Internet Explorer μας παρέχει μόνο μια ειδοποίηση στην γραμμή διευθύνσεων σχετικά με το ενδεχόμενο η συγκεκριμένη τοποθεσία Web να είναι τοποθεσία ηλεκτρονικού ¨ψαρέματος¨

6.2.1.3 Τεχνικές Phishing

6.2.1.3.1 Χειρισμός συνδέσεων (Link manipulation).

Οι περισσότερες μέθοδοι χρησιμοποιούν κάποια μορφή τεχνικής εξαπάτησης με σκοπό να κάνουν μια σύνδεση σε ένα ηλεκτρονικό ταχυδρομείο και ο ¨θήτης¨ Ιστοχώρος που οδηγεί η σύνδεση αυτή εμφανίζεται να ανήκει στην προς εξαπάτηση οργάνωση. Λάθος γραμμένα URLs ή ακόμη η χρήση των subdomains είναι κοινά τεχνάσματα που χρησιμοποιούνται από τα phishers . Στο ακόλουθο παράδειγμα URL μπορούμε να το δούμε αυτό , καθώς η ηλεκτρονική διεύθυνση http://www.yourbank.example.com/, εμφανίζεται σαν το URL το οποίο μας οδηγεί στο τμήμα example του yourbank web site , στην πραγματικότητα όμως το URL οδηγεί στο τμήμα yourbank (i.e phishing) του example web site.

Ένα ακόμη γνωστό τέχνασμα είναι αυτό στο οποίο το κείμενο συνδέσεων anchor , εμφανίζεται να είναι έγκυρο , παρόλο που στην πραγματικότητα η σύνδεση οδηγείται στο phisher site .

Μια παλιά μέθοδος phishing χρησιμοποιούσε συνδέσεις οι οποίες περιείχαν το σύμβολο ¨@¨, το οποίο προοριζόταν αρχικά ως ένας τρόπος για να εισαχθεί κάποιο όνομα χρήστη ή κάποιος κωδικός .
Για παράδειγμα , η σύνδεση http://www.google.com@members.tripod.com ίσως να εξαπατά κάποιον απλό παρατηρητή , εκτιμώντας ότι θα ανοίξει μια σελίδα στο www.google.com στην πραγματικότητα ο browser οδηγείτε σε μια σελίδα member.tripod.com , η οποία χρησιμοποιεί το κωδικό όνομα www.google.com , η σελίδα ανοίγει κανονικά ανεξάρτητα από το παρεχόμενο όνομα του χρήστη . Τέτοιου είδους URL είναι απενεργοποιημένες στον Internet Explorer , ενώ σε αντίθεση στον Mozilla Firefox και στον Opera παρουσιάζεται απλά ένα μήνυμα προειδοποίησης και δίνει το δικαίωμα της επιλογής της συνέχισης ή της ακύρωσης του site .

Ένα ακόμη πρόβλημα με URL εμφανίστηκε στον χειρισμό των IDN στον IE , πιθανά κακόβουλα sites έχουν την δύναμη να επιτρέπουν οπτικά παρόμοιες διευθετήσεις Ιστού να οδηγούν σε διαφορετικές διευθύνσεις ιστού . Παρόλη την δημοσιότητα που διαθέτει αυτού του είδους την ρωγμή , γνωστή και ως **IDN spoofing** ή **Homograph attack** , καμία γνωστή επίθεση phishing δεν την έχει εκμεταλλευτεί ακόμη . Το phishers έχει εκμεταλλευτεί έναν παρόμοιο κίνδυνο , χρησιμοποιώντας ανοιχτά redirectors URL Ιστοχώρων έμπιστων οργανισμών με σκοπό να μεταμφιέσει κακόβουλα URL σε έμπιστα domain.

6.2.1.3.2 Διαφυγή φίλτρων (Filter evasion).

Οι Phishers στη δεύτερη τεχνική phishing έχουν ως στόχο την διαφυγή φίλτρων . Χρησιμοποιούν εικόνες αντί για κείμενο για να κάνουν σκληρότερα τα ant-phishing φίλτρα , έτσι ώστε να μπορεί να ανιχνευτεί το κείμενο που χρησιμοποιείται στα phishing e-mails.

6.2.1.3.3 Παραποίηση Ιστοχώρου (Website forgery).

Η Τρίτη τεχνική phishing , είναι η λεγόμενη παραποίηση Ιστοχώρου . Όταν κάποιο υποτιθέμενο θύμα επισκεφτεί κάποιο website phishing , η εξαπάτηση δεν έχει ολοκληρωθεί . Αρκετές απάτες τύπου phishing χρησιμοποιούν εντολές τύπου JavaScript προκειμένου να μεταπηδήσουν στην γραμμή διευθύνσεων. Αυτό επιτυγχάνεται είτε με την τοποθέτηση κάποιας εικόνας ή ενός μη νόμιμου URL στην θέση του πλαισίου διευθύνσεως , είτε κλείνοντας την αυθεντική διεύθυνση και ανοίγοντας μια εντελώς καινούργια η οποία θα διαθέτει ένα μη νόμιμο URL.
Ένας επιτιθέμενος μπορεί ακόμη να χρησιμοποιήσει τις ρωγμές στα χειρόγραφα ενός εμπιστευτικού Ιστοχώρου ενάντια στο θύμα . Αυτού του είδους ο επιθέσεις , γνωστές και ως **cross-site scripting** , είναι ιδιαίτερα προβληματικές επειδή καθοδηγούν τους χρήστες να υπογράψουν μέσα στις τράπεζες ή τις ιστοσελίδες υπηρεσιών , στα οποία όλα από την διεύθυνση μέχρι και τα πιστοποιητικά ασφαλείας εμφανίζονται ορθά και νόμιμα. Στην πραγματικότητα όμως , η σύνδεση για το αυτό το website είναι τροποποιημένη με τέτοιο τρόπο ώστε να εκκινήσει την επίθεση . Παρόλα αυτά όμως είναι πολύ δύσκολο να σημειωθούν και να κατανοηθούν όλα αυτά χωρίς εξειδικευμένη γνώση .
Πάντως μια τέτοιου είδους ρωγμή χρησιμοποιήθηκε το2006 στο PayPal.

Οι χρήστες από την μεριά τους για να αποφύγουν τις επιθέσεις της τεχνικής anti-phishing , μπορούν να σκανάρουν τους Ιστοχώρους για συσχετιζόμενα κείμενα τύπου phishing, οι Phishers έχουν αρχίσει και εφαρμόζουν πλέον websites βασιζόμενα σε Flash . Αυτά τα site μοιάζουν πολύ με τα κανονικά , με την ιδιαιτερότητα ότι κρύβουν τα κείμενα αυτά σε αντικείμενα πολυμέσα.

6.2.1.3.4 Τηλεφωνικό Phishing (Phone Phishing).

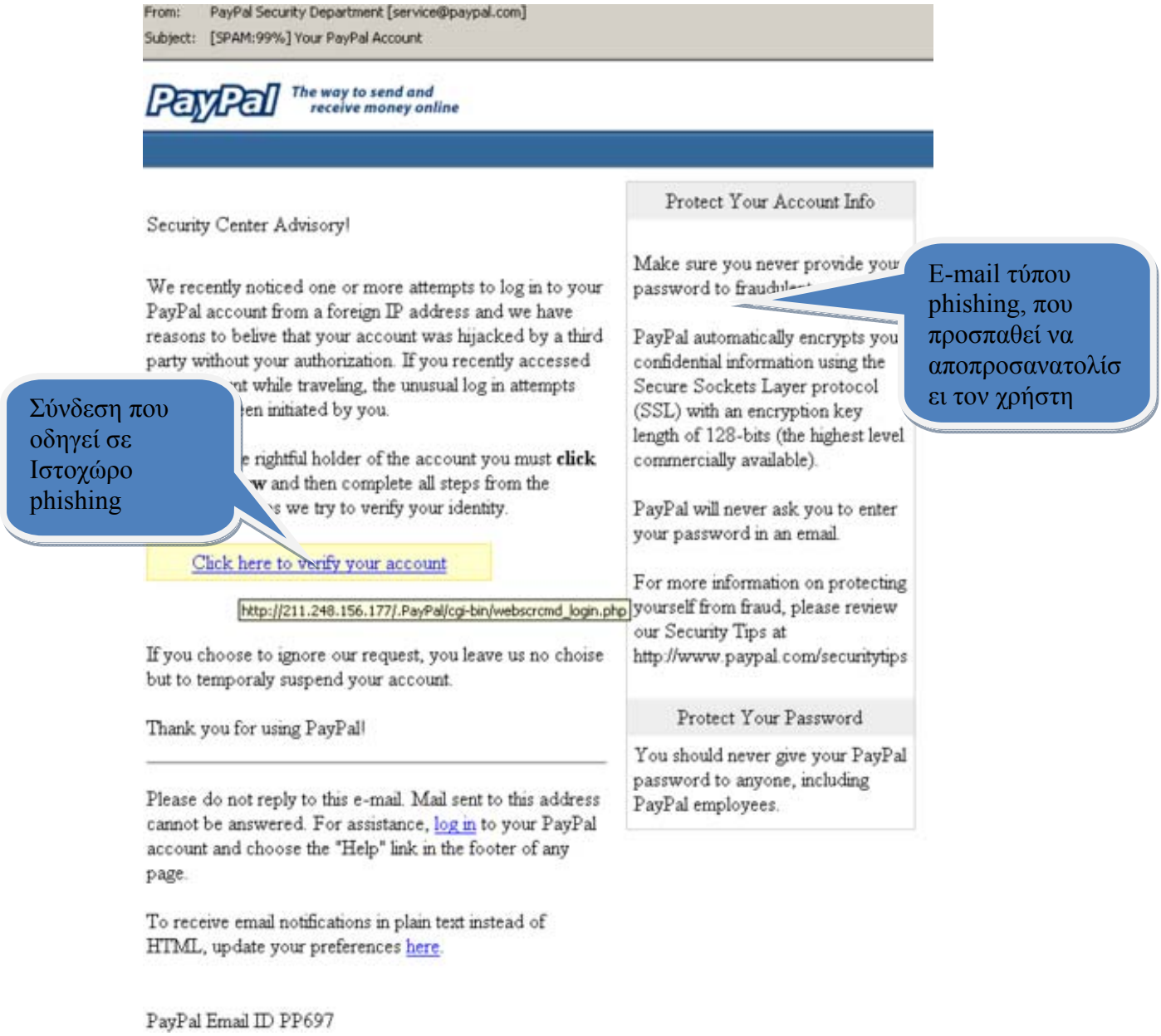
Τέλος έχουμε το τηλεφωνικό phishing , αυτού του είδους η τεχνική σε σχέση με τις προηγούμενες τεχνικές δεν χρησιμοποιεί ψεύτικα site . Ο επιτιθέμενος στέλνει ένα μήνυμα το οποίο δηλώνει ότι είναι από άλλον αποστολέα και προτρέπει την επικοινωνία του θύματος με το θύτη από εκείνο το σημείο και μετά εφαρμόζεται η επίθεση .
Για παράδειγμα έρχεται ένα μήνυμα το οποίο ισχυρίζεται ότι προέρχεται από μια τράπεζα που το θύμα χρησιμοποιεί και προτρέπει τον χρήστη να τηλεφωνήσει σε έναν τηλεφωνικό αριθμό με αιτία κάποιο πρόβλημα που παρουσιάστηκε στον λογαριασμό του χρήστη .
Μόλις το θύμα τηλεφωνήσει στον αριθμό αυτό ο οποίος παρέχεται από την υπηρεσία Voice over IP και ο οποίος ανήκει και στον phisher ο οποίος έχει επιχειρήσει και την επίθεση , του ζητείται να εμφανίσει τον αριθμό του λογαριασμού του και τον κωδικό του, κάποιες φορές τα θύματα πέφτουν στην παγίδα και αποκαλύπτουν τα στοιχεία τους . Μερικές φορές δίνεται και ψεύτική τηλεφωνική ταυτότητα για να εμφανίζεται ότι οι κλήσεις αυτές προορίζονται ή προέρχονται από κάποιο έμπιστο οργανισμό.

6.2.1.4 Παραδείγματα Phishing

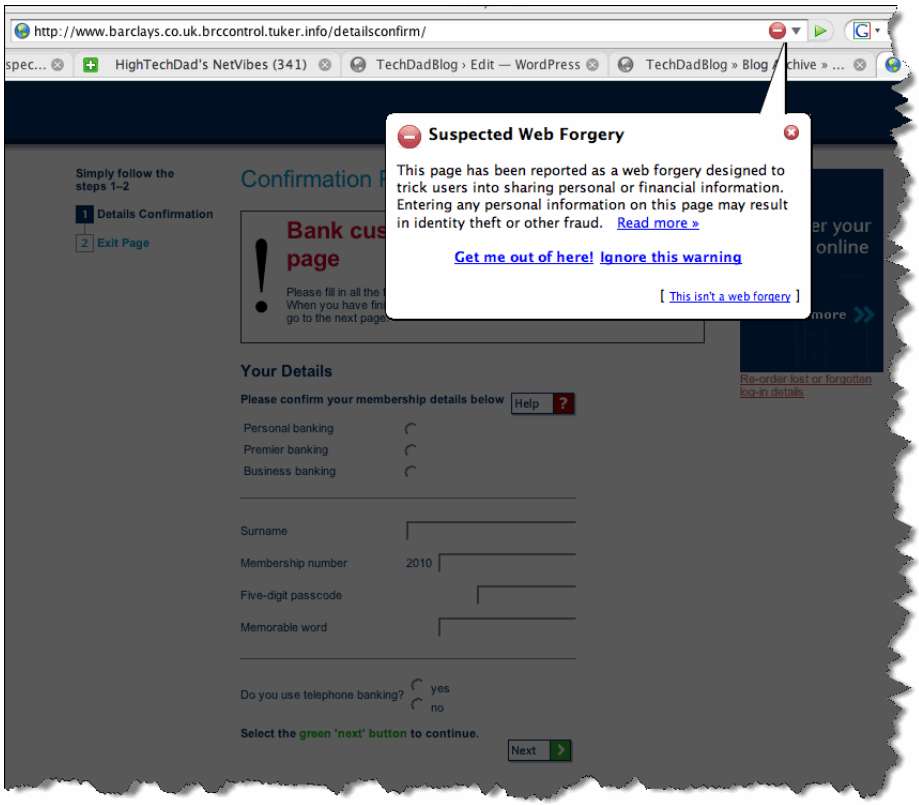
Ένα παράδειγμα Phishing site , το ακόλουθο είναι του οργανισμού PayPal .Ένα έμπειρος χρήστης θα μπορούσε να το αναγνωρίσει από τα ορθογραφικά λάθη που εμφανίζονται στο ηλεκτρονικό ταχυδρομείο , καθώς και η παρουσία μιας διεύθυνσης IP με σύνδεση (που εμφανίζεται μέσα στο πλαίσιο) .Όλα τα προηγούμενα καταδεικνύουν την ύπαρξη του phishing site . Άλλες ενδείξεις είναι η έλλειψη ενός προσωπικού χαιρετισμού , αν και η παρουσία προσωπικών λεπτομερειών δεν θα αποτελούσε εγγυητικό στοιχείο νομιμότητας .
Μια νόμιμη επικοινωνία με τον οργανισμό PayPal θα εμφάνιζε σίγουρα κάποια βασικά στοιχεία όπως κάποιο χαιρετισμό με τον χρήστη ο οποίος θα περιείχε το πραγματικό όνομα του/ της , και όχι έναν γενικό χαιρετισμό όπως ¨Dear Accountholder¨ . Άλλα σημάδια ότι το μήνυμα είναι μια απάτη είναι η λανθασμένη ορθογραφία απλών λέξεων, κακή χρήση της γραμματικής καθώς και η αποτυχία εφαρμογής των απειλών των συνεπειών ,όπως η αναστολή απολογισμού εάν ο παραλήπτης αποτυγχάνει να συμμορφωθεί με τα αιτήματα του μηνύματος κα .

Σημειώνουμε ότι πολλά από τα phishing ηλεκτρονικά ταχυδρομεία θα περιλάβουν , όπως και κάποιο πραγματικό ηλεκτρονικό ταχυδρομείο του οργανισμού PayPal ,προειδοποιήσεις της μορφής να μην εμφανίζουμε τον κωδικό μας και τα προσωπικά μας στοιχεία (με σκοπό να μας παραπλανήσουν) .
Ενημερώνονται επίσης οι χρήστες, για την πιθανότητα που έχουν να δεχτούν επιθέσεις τύπου phishing, ακόμη μέσω τον κακόβουλων αυτών site παρέχονται συνδέσεις προς Ιστοχώρους οι οποίοι παρέχουν πληροφορίες και οδηγίες σχετικές με το πώς μπορούν οι χρήστες να αποφύγουν τέτοιου είδους απειλές . Όλα τα παραπάνω είναι μέρη όλων αυτών που καθιστούν τα phishing sites και τα phishing ηλεκτρονικά ταχυδρομεία τόσο παραπλανητικά .

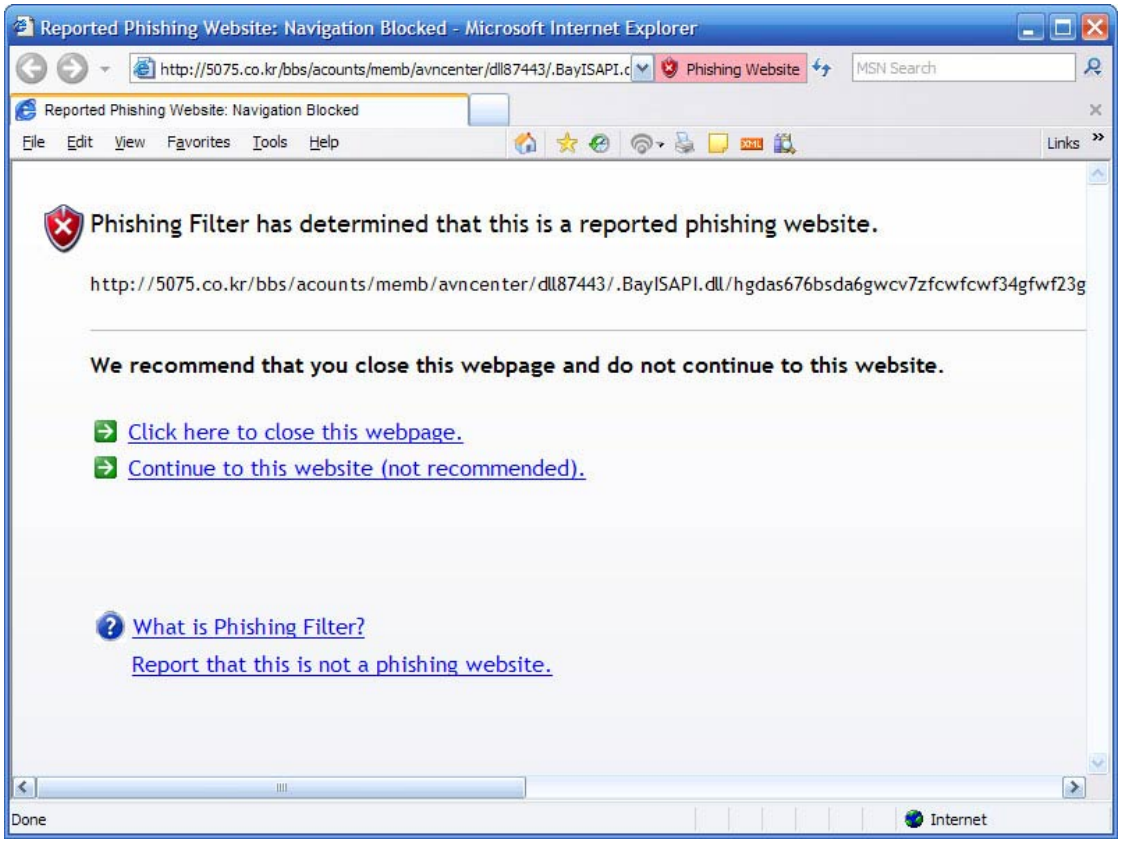
Στο παράδειγμα που ακολουθεί , υπάρχει ηλεκτρονικό ταχυδρομείο τύπου phishing , το οποίο προειδοποιεί τον χρήστη ότι τα ηλεκτρονικά ταχυδρομεία από τον οργανισμό PayPal δεν ζητάνε ποτέ τις ευαίσθητες πληροφορίες και τα προσωπικά δεδομένα του χρήστη. Γεγονός που όντως ισχύει , σε αντίθεση όμως, παροτρύνει τον χρήστη να ακολουθήσει μια σύνδεση προκειμένου να επιβεβαιώσει τον λογαριασμό του . Σε περίπτωση που ο χρήστης ακολουθήσει την διεύθυνση αυτή μεταφέρεται σε έναν περαιτέρω Ιστοχώρο που κατασκευάζεται να μοιάζει με αυτόν του οργανισμού PayPal, και εκεί του ζητούνται να δώσει τις ευαίσθητες πληροφορίες του .



Εικόνα 36: Παράδειγμα 1ο Ιστοχώρος Phishing PayPal.

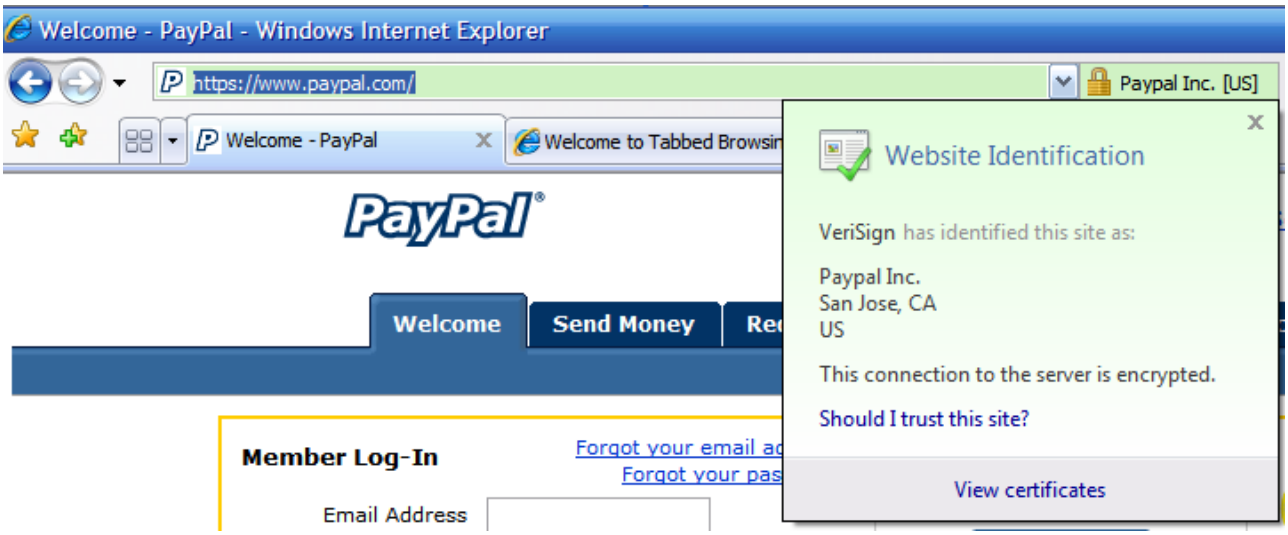


Εικόνα 37: Παράδειγμα 2ο Ιστοχώρος Phishing Barclays .



Εικόνα 38 : Παράδειγμα 3ο Ιστοχώρος Phishing.

Εικόνα 39 : Παράδειγμα 4ο Υπόδειξη Ιστοχώρου Phishing .



Εικόνα 40 : Παράδειγμα 5ο Υπόδειξη Ιστοχώρου Phishing .

6.2.1.5 Τεχνικές καταπολέμησης του Phishing .

Υπάρχουν αρκετά διαφορετικές τεχνικές καταπολέμησης του phishing , συμπεριλαμβανομένου της νομοθεσίας και της τεχνολογίας που έχουν δημιουργηθεί συγκεκριμένα για αυτόν τον λόγο :

- **Μέσω των χρηστών** : Ένας τρόπος αντιμετώπισης του phishing είναι να εκπαιδεύσουμε τους χρήστες με τέτοιο τρόπο που να αναγνωρίζουν τις επιθέσεις αυτού του είδους και να μπορούν έτσι να τις αντιμετωπίσουν . Η εκπαίδευση μπορεί να αποβεί πολύ αποτελεσματική ειδικά όταν παρέχεται άμεσα και ακολουθεί και συνεχής μετεκπαίδευση .

- **Μέσω των τεχνικών μέσων** : Τα αντί-phishing μέτρα έχουν αναγνωριστεί και καθιερωθεί ως χαρακτηριστικά γνωρίσματα των μηχανών αναζήτησης , ενσωματώνονται στις μηχανές αυτές ως επιπρόσθετα εργαλεία . Αποτελούν με αυτόν ον τρόπο έναν από τους κύριους τρόπους αντιμετώπισης του Phishing.

  a) **Μέσω της αναγνώρισης των Phishing websites** : Τον καιρό που το phishing βασιζότανε στην προσωποποίηση , η παρεμπόδισή του εξαρτιόταν σε κάποιος αξιόπιστους τρόπους οι οποίοι καθόριζα την πραγματική ταυτότητα του εκάστοτε Ιστοχώρου . Για παράδειγμα , κάποιες αντί-phishing εργαλειοθήκες εμφάνιζαν το domain name των επισκεπτόμενων Ιστοχώρων .

  b) **¨Δυσκολεύοντας ¨ τους κωδικούς των εισόδων :** Πολλές εταιρίες και οργανισμοί , προτρέπουν τους χρήστες τους να εισάγουν πιο δύσκολους κωδικούς εισόδου ,με διάφορες ιδιαιτερότητες . Για παράδειγμα μια τράπεζα στις Ηνωμένες Πολιτείες ζητούσε από τους πελάτες τις , να επιλέξουν εκτός από τον κωδικό και μια ατομική φωτογραφία για την οποία και έπρεπε να πληκτρολογούν ,σε μετέπειτα προσπάθειές τους να μπουν στους προσωπικούς τους λογαριασμούς , κάποιον ειδικό κωδικό . Κάθε φορά που η τράπεζα τους εμφάνιζε την φωτογραφία αυτή , οι χρήστες έπρεπε να παρέχουν τον κωδικό αυτό .

  c) **Οι μηχανές αναζήτησης προειδοποιούν τους χρήστες για τους ψευδείς Ιστοχώρους:** Μια άλλη δημοφιλής μέθοδος αντιμετώπισης του phishing είναι αυτή μέσω των μηχανών αναζήτησης ,οι οποίες διατηρούν έναν κατάλογο γνωστών phishing περιοχών και κάθε φορά ελέγχουν το είδος των Ιστοχώρων με βάση τον κατάλογο αυτό. Αυτό το μέτρο καταπολέμησης του phishing εμπεριέχεται στους ακόλουθους browser , Microsoft IE7, Mozilla Firefox και στον Opera.

  d) **Εξάλειψη των phishing e-mails:** Η τελευταία υποκατηγορία της αντιμετώπισης του phishing μέσω τεχνικών μέσω , είναι αυτή της εξάλειψης των phishing e-mails . Στην τεχνική αυτή εξειδικευμένα φίλτρα spam μπορούν να μειώσουν τον αριθμό των ηλεκτρονικών μηνυμάτων που φτάνουν στα εισερχόμενα των χρηστών . Η τεχνική αυτή στηρίζεται σε μια μέθοδος ταξινόμησης των phishing e-mails , αναγνωρίζονται δηλαδή

αυτού του είδους τα ηλεκτρονικά μηνύματα και αποτρέπονται προτού φτάσουν στους χρήστες.

6.2.1.6 Πώς θα ξέρω εάν μια ηλεκτρονική συναλλαγή μου είναι ασφαλής ;

6.2.1.6.1 Τι είναι μια ασφαλής σύνδεση .

Μια ασφαλής σύνδεση είναι μια κρυπτογραφημένη ανταλλαγή πληροφοριών μεταξύ μιας τοποθεσίας Web την οποία επισκεπτόμαστε και του Internet Explorer . Η κρυπτογράφηση παρέχεται μέσω ενός εγγράφου το οποίο η τοποθεσία Web και το οποίο ονομάζεται πιστοποιητικό .Όταν αποστέλλουμε πληροφορίες στην τοποθεσία Web , αυτές κρυπτογραφούνται στον υπολογιστή μας και αποκρυπτογραφούνται στην τοποθεσία Web. Υπό κανονικές συνθήκες , η ανάγνωση ή η αλλοίωση των πληροφοριών δεν είναι δυνατή κατά την αποστολή τους , ωστόσο , υπάρχει η πιθανότητα κάποιος να ανακαλύψει έναν τρόπο για να σπάσει την κρυπτογράφηση .
Ακόμη και αν η σύνδεση μεταξύ του υπολογιστή μας και της τοποθεσίας Web είναι κρυπτογραφημένη , αυτό δεν εγγυάται ότι η τοποθεσία Web είναι αξιόπιστη .Το ιδιωτικό μας απόρρητο εξακολουθεί να διατρέχει κίνδυνο από τον τρόπο με τον οποίον η τοποθεσία Web χρησιμοποιεί η διανέμει τις πληροφορίες μας .

6.2.1.6.2 Πως βλέπω εάν έχω ασφαλή σύνδεση .

Παρά το γεγονός ότι οι πληροφορίες που στέλνονται μεταξύ της τοποθεσίας Web την οποία επισκεπτόμαστε και του Internet Explorer είναι κρυπτογραφημένες ,ένα ενδιάμεσο μέρος ενδέχεται να μπορεί να εντοπίσει την τοποθεσία Web στην οποία συνδεόμαστε . Γνωρίζοντας την τοποθεσία στην οποία συνδεόμαστε , το άλλο μέρος ενδέχεται να διαμορφώσει μια ακριβή άποψη του τι κάνουμε στην συγκεκριμένη τοποθεσία.

Από την μεριά μας τώρα και για την μεγαλύτερη ασφάλειά μας θα πρέπει να γνωρίζουμε ένα έχουμε μια ασφαλή σύνδεση . Αυτό πετυχαίνεται με το να παρακολουθούμε τα ειδικά εικονίδια ή χρώματα που εμφανίζονται στον Internet Explorer .

Εάν στον Internet Explorer δούμε ένα εικονίδιο λουκέτο () στην γραμμή κατάστασης ασφάλειας , η οποία γραμμή βρίσκεται στην δεξιά πλευρά της γραμμής διευθύνσεων , τότε η σύνδεσή μας είναι ασφαλής .

Το πιστοποιητικό το οποίο χρησιμοποιείται για την κρυπτογράφηση της σύνδεσης περιέχει επίσης πληροφορίες σχετικά με την ταυτότητα του κατόχου ή της εταιρείας της τοποθεσίας Web . Μπορούμε να κάνουμε κλικ στο εικονίδιο κλειδαριά για να προβάλουμε την ταυτότητα της τοποθεσίας αυτής.

Σε περίπτωση τώρα που επισκεπτόμαστε μια τοποθεσία Web η οποία χρησιμοποιεί ασφαλή σύνδεση , το χρώμα της γραμμής κατάστασης ασφάλειας μας υποδεικνύει εάν το πιστοποιητικό είναι έγκυρο και εμφανίζει το επίπεδο επικύρωσης που πραγματοποιήθηκε από τον οργανισμό πιστοποίησης .

Ο πίνακας που ακολουθεί περιγράφει την σημασία των χρωμάτων της γραμμής κατάστασης ασφαλείας .

Πίνακας 3 : Περιγραφή της σημασίας των χρωμάτων της γραμμής κατάστασης ασφαλείας .

Περιγραφή της σημασίας των χρωμάτων της γραμμής κατάστασης ασφαλείας .	
Έγχρωμη	**Τι σημαίνει**
Κόκκινο	Το πιστοποιητικό έχει λήξει , δεν είναι έγκυρο ή περιέχει σφάλμα .
Κίτρινο	Δεν είναι δυνατή η επιβεβαίωση της γνησιότητας του πιστοποιητικού ή της αρχής έκδοσης του πιστοποιητικού που το εξέδωσε.
Λευκό	Το πιστοποιητικό διαθέτει κανονική επικύρωση . Αυτό σημαίνει ότι η επικοινωνία μεταξύ του προγράμματος περιήγησης και της τοποθεσίας Web είναι κρυπτογραφημένη .Η αρχή έκδοσης πιστοποιητικών δεν παρέχει καμία διαβεβαίωση σχετικά με τις επιχειρηματικές πρακτικές της τοποθεσίας Web.
Πράσινο	Το πιστοποιητικό χρησιμοποιεί εκτεταμένη επικύρωση. Αυτό σημαίνει ότι η επικοινωνία μεταξύ του προγράμματος περιήγησης και της τοποθεσίας Web είναι κρυπτογραφημένη και η αρχή έκδοσης πιστοποιητικών επιβεβαίωσε ότι η τοποθεσία Web ανήκει ή λειτουργεί από επιχείρηση η οποία έχει συσταθεί νομικά σύμφωνα με την δικαιοδοσία που φαίνεται στο πιστοποιητικό και την γραμμή κατάστασης ασφαλείας . .Η αρχή έκδοσης πιστοποιητικών δεν παρέχει καμία διαβεβαίωση σχετικά με τις επιχειρηματικές πρακτικές της τοποθεσίας Web.

Σε περίπτωση τώρα που πιστεύουμε ότι μια τοποθεσία προσπαθεί να μας παραπλανήσει σχετικά με την ταυτότητά της , θα πρέπει να επικοινωνήσουμε με την αρχή έκδοσης πιστοποιητικών το όνομα της οποίας εμφανίζεται στο πιστοποιητικό και στην γραμμή κατάστασης ασφαλείας .

7 ΕΠΙΠΛΕΟΝ ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΤΩΝ WINDOWS VISTA.

7.1 Γονικός Έλεγχος – User Account Control

Ένα άλλο χαρακτηριστικό ασφάλειας που συνεισφέρει στην πληρότητας της αρχιτεκτονικής ασφαλείας των Windows Vista είναι και ο **Γονικός έλεγχος (User Account Control)**. Το User Account Control , είναι μια νέα λειτουργία των Windows που αποτρέπει τις αυθαίρετες ενέργειες στον υπολογιστή μας . Είναι ένας μηχανισμός ο οποίος δίνει σε κάθε χρήστη ξεχωριστά το δικαίωμα της πρόσβασης ή όχι σε διάφορες πτυχές του σύστημά μας .
Εδώ πρέπει να τονίσουμε ότι όταν αναφέρουμε την πρόσβαση ή όχι δεν εννοούμε σε απλά αρχεία , αλλά το δικαίωμά της πρόσβασης μας σε διάφορες περιοχές του λειτουργικού συστήματος.
Σε διαφορετικά σύνολα ρυθμίσεων μπορεί να επέμβει ο απλός χρήστης (user) και σε διαφορετικά ο διαχειριστής (administrator) .
Ένας απλός χρήστης, για παράδειγμα , δεν μπορεί να αλλάξει τις ρυθμίσεις του οδηγού για την κάρτα γραφικών , ούτε να επέμβει στις ρυθμίσεις του τοίχους προστασίας (firewall).
Ο μηχανισμός αυτός έχει διάφορες ονομασίες όπως μηχανισμός δικαιωμάτων ή User Account Control ή απλά UAC.
Ο μηχανισμός αυτός καθιστά ικανούς τους χρήστες να εκτελέσουν κοινές εργασίες είτε ως απλοί-τυποποιημένοι χρήστες , όπως ονομάζονται στα Windows Vista, είτε ως διαχειριστές χωρίς να χρειάζεται
να αλλάζουν οι χρήστες , δηλαδή χωρίς να χρειάζεται να κάνουν log-off καθώς τρέχουν στο σύστημα .

Ο απλός χρήστης είναι συνώνυμο του λογαριασμού χρήστη των Windows XP. Οι λογαριασμοί χρηστών είναι αυτοί των οποίων τα μέλη μπορούν να τρέχουν τις περισσότερες εφαρμογές σαν τυποποιημένοι χρήστες . Ο UAC χαρακτηρίζεται σαν ένα πολύ σημαντικό χαρακτηριστικό των Windows Vista και αυτό γιατί έχει την ικανότητα να ξεχωρίζει τις λειτουργίες του διαχειριστή από αυτές του απλού χρήστη και αυτό έχει σαν αποτέλεσμα την ενίσχυση της παραγωγικότητας των χρηστών .

7.1.1 Περιγραφή του UAC

Η λειτουργία του UAC είναι απλή, κάθε φορά που κάποιος χρήστης επιθυμεί να επέμβει σε μια ευαίσθητη περιοχή γίνεται έλεγχος των δικαιωμάτων του χρήστη . Ελέγχεται δηλαδή εάν είναι εξουσιοδοτημένος ο χρήστης για αυτήν την ενέργεια ή όχι. Με τον τρόπο αυτό προλαμβάνετε τόσο η εγκατάσταση κακόβουλων στοιχείων όπως malware και spyware όσο και η πραγματοποίηση αλλαγών που θα μπορούσαν να επηρεάσουν τόσο εμάς όσο και άλλους χρήστες του υπολογιστή αυτού .

Αναλυτικά τώρα, όταν ένας Διαχειριστής εισέρχεται σε ένα σύστημα που διαθέτει Windows Vista , ο χρήστης αυτός ορίζεται από δύο διαφορετικά σημεία πρόσβασης (access token).

Τα σημεία αυτά πρόσβασης περιέχουν πληροφορίες ,για τα μέλη του γκρουπ του χρήστη , στοιχεία επικύρωσης καθώς και δεδομένα ελέγχου πρόσβασης , όλα αυτά τα στοιχεία χρησιμοποιούνται από τα Windows προκειμένου να ελέγξουν σε ποιους πόρους και σε ποιες εργασίες έχει ο εκάστοτε χρήστης πρόσβαση.

Προτού τα Windows Vista , ένας λογαριασμός διαχειριστή λάμβανε ένα σημείο πρόσβασης το οποίο περιείχε δεδομένα τα οποία χορηγούσαν την πρόσβαση του χρήστη σε όλους τους πόρους του συστήματος .Αυτό το μοντέλο πρόσβασης δεν συμπεριλάμβανε κανένα έλεγχο αποτυχίας-ασφάλειας για να διασφαλίσει ότι όντως οι χρήστες θέλησαν αληθινά να εκτελέσουν μια εργασία η οποία απαιτεί το διοικητικό σημείο πρόσβασης .
Ας αποτέλεσμα κακόβουλα λογισμικά της μορφής όπως τα malware , μπορούσαν να εγκατασταθούν ανενόχλητα στα συστήματα των χρηστών ,χωρίς να γίνεται αντιληπτό καθόλου από τους χρήστες αυτό το γεγονός . Η διαδικασία αυτή είναι γνωστή και ως ¨αθόρυβη¨ εγκατάσταση.
Με ακριβώς την ίδια μέθοδο ένα malware μπορεί αν εγκατασταθεί και σε έναν λογαριασμό διαχειριστή αντίστοιχα . Οι ζημιές οι οποίες μπορούν να προκληθούν σε αυτήν την περίπτωση είναι πολύ περισσότερες γιατί το κακόβουλο λογισμικό μπορεί να εκμεταλλευτεί τα δεδομένα του ελέγχου πρόσβασης του διαχειριστή και να επηρεάσει έτσι τα αρχεία του πυρήνα του λειτουργικού μας συστήματος , ενέργειες που σε μερικές περιπτώσεις είναι σχεδόν αδύνατον να αναιρεθούν.

Η πρωταρχική διαφορά ανάμεσα σε ένα απλό χρήστη και σε ένα διαχειριστή , στα Windows Vista είναι τα επίπεδα πρόσβασης που οι χρήστες έχουν εκτός από τον πυρήνα και στις προστατευμένες περιοχές του υπολογιστή . Οι διαχειριστές έχουν την δυνατότητα να αλλάξουν την κατάσταση του συστήματος , να θέσουν εκτός λειτουργίας το firewall , να διαμορφώσουν τις πολιτικές ασφάλειας, να εγκαταστήσουν κάποια υπηρεσία ή κάποιον οδηγό(driver) , πράγματα τα οποία μπορούν να επηρεάσουν κάθε χρήστη του συστήματος και να εγκαταστήσουν κακόβουλα λογισμικά σε ολόκληρο το σύστημα.

Για την πρόληψη των αθόρυβων εγκαταστάσεων των malware καθώς και την αποφυγή των μολύνσεων από την πλευρά του υπολογιστή , τα Microsoft ανέπτυξαν τον νέο αυτό χαρακτηριστικό των Windows Vista , UAC .
Αντίθετα με τις προηγούμενες εκδόσεις των Windows ,όπως προαναφέραμε , όταν ένας διαχειριστής εισέρχεται στο σύστημα , το σημείο πλήρους πρόσβαση χωρίζεται σε δύο σημεία πρόσβασης : 1) σε ένα πλήρους διαχειριστή σημείο πρόσβασης και 2) σε ένα σημείο πρόσβασης τυπικού χρήστη.
Κατά την διάρκεια της διαδικασίας log on , τα συστατικά της επικύρωσης και του ελέγχου πρόσβασης , τα οποία προσδιορίζουν ένα διαχειριστή τίθενται εκτός λειτουργίας με αποτέλεσμα να καταλήγει σε τυποποιημένου χρήστη σημείο πρόσβασης .
Όταν ένας χρήστης-διαχειριστής εισέρχεται στο σύστημα όλες οι εφαρμογές κληρονομούν τα δεδομένα ελέγχου πρόσβασης με την αρχική έναρξη της επιφάνειας εργασίας , οι εφαρμογές αυτές μπορούν να χρησιμοποιηθούν ταυτόχρονα και από έναν τυποποιημένο χρήστη , χωρίς απαιτείται καμία αλλαγή.

Σε αντίθεση με αυτήν την διαδικασία , όταν ένας τυποποιημένος χρήστης εισέρχεται στο σύστημα , δημιουργείται μόνο ένα σημείο τυποποιημένου χρήστη σημείο πρόσβασης . Αυτό το σημείο πρόσβασης είναι αυτό που στην συνέχεια χρησιμοποιείται και από τις εφαρμογές με την έναρξη της επιφάνειας εργασίας.

Μετά την είσοδο ενός διαχειριστή το σημείο πλήρους πρόσβασης διαχειριστή μένει ανενεργό μέχρι ο χρήστης να επιχειρήσει να εκτελέσει μια εργασία με διαχειριστικές απαιτήσεις. Επειδή η

εμπειρία του χρήστη διαμορφώνεται ανάλογα με το μοντέλο διαχείρισης των πολιτικών ασφαλείας του συστήματος (secpol.msc) , καθώς επίσης και από το σύνολο των πολιτικών που εφαρμόζονται στο σύστημα (gpedit.msc) , δεν υπάρχει μια μοναδική

Έστω ότι ένας απλός χρήστης επιθυμεί να επέμβει σε κάποια ρύθμιση του συστήματος, του ζητάτε από το σύστημα ,το συνθηματικό (password) του διαχειριστή με αυτόν τον τρόπο γίνεται διαπίστωση εάν είναι εξουσιοδοτημένος ή όχι
Στην περίπτωση τώρα που ο χρήστης έχει δικαιώματα administrator , η προσπάθειά του να επέμβει σε κάποια ρύθμιση του συστήματος , πάλι θα θορυβήσει το λειτουργικό σύστημα , ωστόσο όμως την φορά αυτή , δεν θα του ζητηθεί , ούτε θα χρειαστεί να εισάγει κανένα συνθηματικό.
Το λειτουργικό σύστημα θα του ζητήσει απλά μια επιβεβαίωση και εφόσον αυτός την δεκτή θα προχωρήσει κανονικά .

Οι ρυθμίσεις του συστήματος μας που απαιτούν δικαιώματα administrator διαφέρουν και γίνονται εύκολα αντιληπτές από τις υπόλοιπες . Δίπλα στο σχετικό κουμπί ή σύνδεσμο εμφανίζεται μια μικρή ασπίδα με τα χρώματα των windows . Είναι τα εμβλήματα του security center ανάλογα με το χρώμα της ασπίδας πρέπει να εκτελέσουμε και την αντίστοιχη ενέργεια.

- **Τα Windows χρειάζονται την άδεια σας για να συνεχίσουν.**


Μια λειτουργία ή πρόγραμμα των Windows που μπορεί να επηρεάσει άλλους χρήστες αυτού του υπολογιστή χρειάζεται την άδεια σας για να ξεκινήσει. Ελέγξτε το όνομα της ενέργειας για να διασφαλίσετε ότι είναι μια λειτουργία ή πρόγραμμα που θέλετε να εκτελέσετε.

- **Ένα πρόγραμμα χρειάζεται την άδεια σας για να συνεχίσει.**


Ένα πρόγραμμα που δεν αποτελεί μέρος των Windows χρειάζεται την άδεια σας για να ξεκινήσει . Έχει έγκυρη ψηφιακή υπογραφή που δηλώνει το όνομα και τον εκδότη του , που συμβάλλει ώστε να διασφαλιστεί ότι το πρόγραμμα είναι αυτό που υποστηρίζεται ότι είναι . Βεβαιωθείτε ότι αυτό είναι ένα πρόγραμμα που θέλετε να εκτελέσετε.

- **Ένα άγνωστο πρόγραμμα ζητά πρόσβαση στον υπολογιστή σας.**


Ένα άγνωστο πρόγραμμα είναι ένα πρόγραμμα που δεν έχει έγκυρη ψηφιακή υπογραφή από τον εκδότη του για να διασφαλίζεται ότι το πρόγραμμα είναι αυτό που υποστηρίζετε ότι είναι . Αυτό δεν δηλώνει απαραίτητα κίνδυνο , καθώς και πολλά παλαιότερα ,νόμιμα προγράμματα δεν έχουν υπογραφές . Ωστόσο θα πρέπει να προσέχετε ιδιαίτερα και να επιτρέπετε αυτό το πρόγραμμα να εκτελείτε μόνο εάν το έχετε λάβει από αξιόπιστη προέλευση , όπως το πρωτότυπο CD ή την τοποθεσία Web ενός εκδότη.

- **Αυτό το πρόγραμμα έχει αποκλειστεί .**


Πρόκειται για ένα πρόγραμμα που έχει αποκλείσει ειδικά ο διαχειριστής σας ώστε να μην εκτελείτε στον υπολογιστή σας . Για να εκτελέσετε αυτό το πρόγραμμα , πρέπει να επικοινωνήσετε με τον διαχειριστεί σας και να ζητήσετε να καταργηθεί ο αποκλεισμός του προγράμματος.

7.1.2 Κατανόηση λογαριασμών χρήστη.

Στα Microsoft Windows XP, ένας χρήστης που θέλει να πραγματοποιήσει ορισμένες κοινές εργασίες όπως την αλλαγή ρυθμίσεων τροφοδοσίας σε έναν φορητό υπολογιστή ή να εγκαταστήσει και να ενημερώσει λογισμικό, πρέπει να είναι ¨διαχειριστής¨ . Ένας από τους λόγους για τους οποίους απαιτούνται δικαιώματα διαχειριστή είναι η προστασία των υπολογιστών από επιβλαβή στοιχεία λήψεις κακόβουλου κώδικα ή κώδικα που έχει δημιουργηθεί με κακοπροαίρετη πρόθεση . Ο κώδικας που έχει δημιουργηθεί με κακοπροαίρετη πρόθεση αφορά ανεπιθύμητο λογισμικό συμπεριλαμβανομένων των ιών τύπου worm , του λογισμικού ανεπιθύμητων διαφημίσεων και του λογισμικού υποκλοπών spyware που θα μπορούσε να διαγράψει ή να κλέψει αρχεία και πληροφορίες από τον υπολογιστή.

Εντούτοις αυτός ο τρόπος λειτουργίας διατηρεί τον υπολογιστή μας πιο ασφαλή ,αλλά παράλληλα περιορίζει την παραγωγικότητα των χρηστών , επειδή κάθε φορά που ένας τυπικός χρήστης χρειάζεται να αλλάξει μια βασική ρύθμιση ή να εγκαταστήσει λογισμικό , θα πρέπει να αναζητά κάποιον χρήστη με δικαιώματα διαχειριστή για να τον βοηθήσει.

Τα Windows Vista μειώνουν τα μειονεκτήματα αυτά παρέχοντας το ίδιο επίπεδο ασφάλειας και όλα αυτά προσφέρονται μέσω του ελέγχου λογαριασμού χρήστη (UAC) , ο οποίος καθιστά ευκολότερη την χρήση ενός υπολογιστή με τυπικά δικαιώματα χρήστη . Μπορούμε να δημιουργήσουμε ξεχωριστούς λογαριασμούς για τον εαυτό μας καθώς και για τους άλλους χρήστες του υπολογιστή μας και να ρυθμίσουμε εύκολα παραμέτρους ασφαλείας για κάθε χρήστη σε κάθε λογαριασμό, για τον έλεγχο των τοποθεσιών Web και των προγραμμάτων στα οποία κάθε χρήστης μπορεί να έχει πρόσβαση και να εγκαθιστά οτιδήποτε χωρίς να απαιτείται πρόσθετη υποστήριξη IT . Επιπλέον , ακόμη και όταν χρησιμοποιούμε έναν λογαριασμό διαχειριστή , θα εξακολουθούμε να επωφελούμαστε από την δυνατότητα βελτιωμένης ασφάλειας . Τα περισσότερα προγράμματα εκτελούνται με τυπικά δικαιώματα χρήστη από προεπιλογή , ακόμη και όταν έχουμε συνδεθεί στον υπολογιστή ως διαχειριστής , γεγονός που περιορίζει τις πιθανές ζημιές από κακόβουλα λογισμικά.

Στα Windows Vista ο τύπος του λογαριασμού χρήστη που διαθέτει ο κάθε χρήστης καθορίζει και τα δικαιώματα που αυτός διαθέτει . Σε αυτό το σημείο είναι απαραίτητο να γίνει μια λεπτομερή παρουσίαση έτσι ώστε να κατανοηθούν πλήρως οι τύποι των χρηστών στα Windows Vista καθώς επίσης και τα δικαιώματα που αυτοί διαθέτουν . Υπάρχουν 3 τύποι λογαριασμών :

A. Λογαριασμός διαχειριστή :

Ένας λογαριασμός διαχειριστή δημιουργείτε κατά την εγκατάσταση των Windows Vista . Ό λογαριασμός αυτός μας παρέχει πλήρη πρόσβαση στον υπολογιστή . Ο διαχειριστής μπορεί να αποκτήσει πρόσβαση τόσο στα δικά του αρχεία όσο και σε λογαριασμούς άλλων χρηστών .

B. Τυπικός λογαριασμός χρήστη :

Ένας τυπικός λογαριασμός χρήστη μας επιτρέπει να εκτελούμε κοινές εργασίες και να εργαζόμαστε με τα δικά μας αρχεία αλλά δεν μπορούμε να βλέπουμε τα αρχεία άλλων χρηστών ή να αλλάξουμε τις ρυθμίσεις τους .

C. Επισκέπτης:

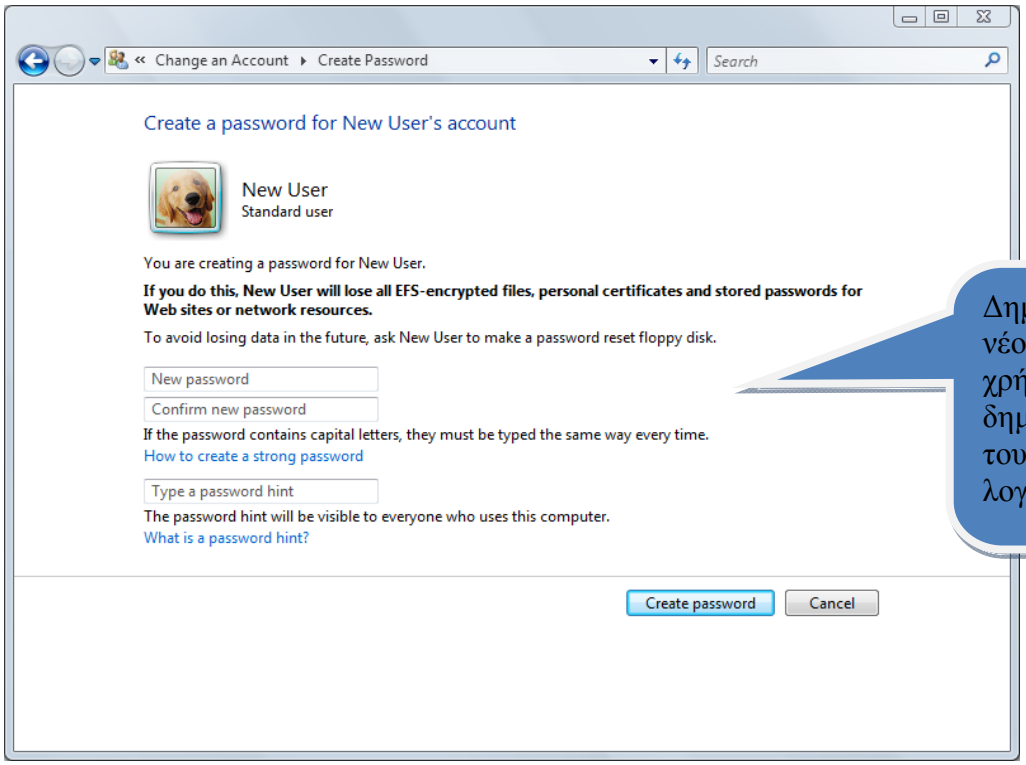
Ένας λογαριασμός επισκέπτη , είναι ένας λογαριασμός για χρήστες που δεν έχουν μόνιμο λογαριασμό στον υπολογιστή . Επιτρέπει στους χρήστες αυτούς να χειρίζονται τον υπολογιστή αλλά δεν τους δίνει πρόσβαση σε αρχεία άλλων χρηστών . Οι επισκέπτες δεν έχουν ο δικαίωμα ούτε να εγκαταστήσουν κάποιο λογισμικό ή υλικό ή έστω να δημιουργήσουν έναν κωδικό πρόσβασης.

7.1.2.1 Δημιουργία νέου λογαριασμού χρήστη

Μπορούμε να δημιουργήσουμε ξεχωριστούς λογαριασμούς για κάθε άτομο που θα χρησιμοποιεί τον υπολογιστή . Αυτό επιτρέπει σε κάθε χρήστη να έχει τους δικούς του φακέλους εγγράφων και τις δικές του προσωπικές ρυθμίσεις , όπως η ταπετσαρία , το μενού Έναρξης , το οπτικό στυλ κ.λπ. Μπορούμε ,ακόμη , να δημιουργήσουμε και να ρυθμίσουμε τις παραμέτρους λογαριασμών χρήστη με το εργαλείο ¨**Λογαριασμοί χρηστών (User Accounts)**¨ στον Πίνακα ελέγχου (Control Panel).
Για να ανοίξουμε το εργαλείο **Λογαριασμοί χρηστών (User Accounts)** , ανοίγουμε τον **Πίνακα Ελέγχου (Control Panel)** από το μενού **Έναρξη (Start)** και κατόπιν κάνουμε διπλό κλικ στο εικονίδιο **Λογαριασμοί χρηστών (User Accounts)** .

Τα βήματα που πρέπει να ακολουθήσουμε για να δημιουργήσουμε έναν νέο χρήστη είναι τα ακόλουθα :

1. Κάνουμε κλικ στο στοιχείο **Δημιουργία νέου λογαριασμού (Create a new account)** στο πλαίσιο λίστας **Επιλογή μιας εργασίας (Pick a task) .**
2. Πληκτρολογούμε το όνομα που θέλουμε να χρησιμοποιήσουμε για τον λογαριασμό και στην συνέχεια κάνουμε κλικ στο κουμπί **Επόμενο (Next) .**
3. Τέλος επιλέγουμε τον τύπο του λογαριασμού που θέλουμε και κατόπιν κάνουμε κλικ στο κουμπί **Δημιουργία λογαριασμού (Create Accounts).**



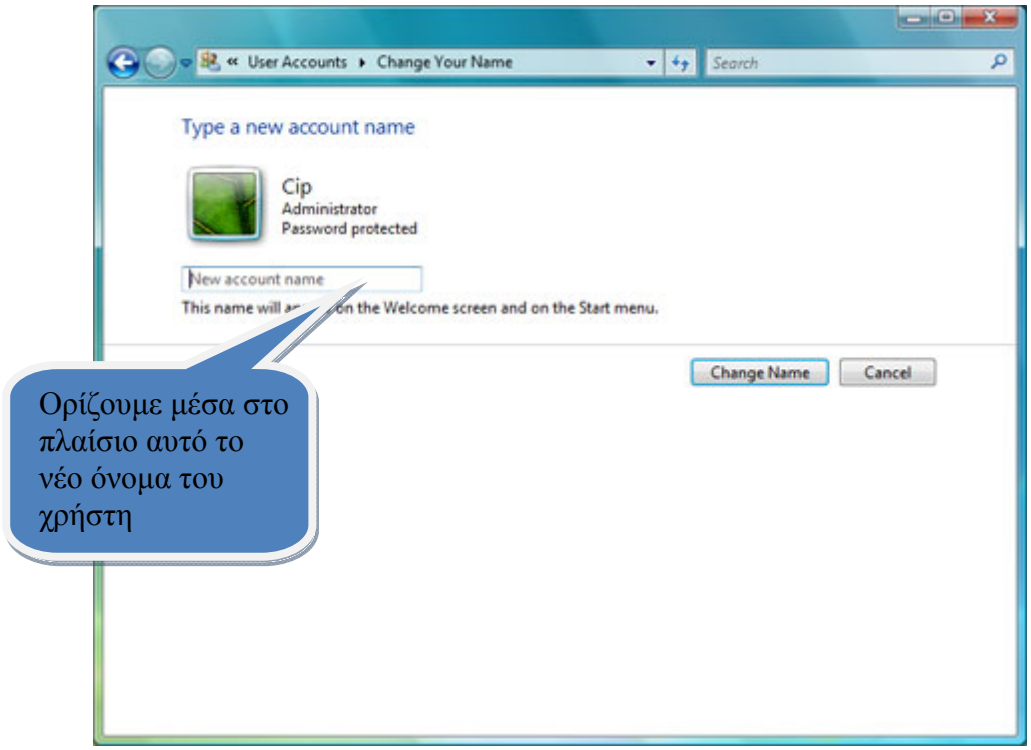
Εικόνα 41: Παράθυρο δημιουργίας νέου λογαριασμού χρήστη.

7.1.2.2 Τροποποίηση λογαριασμού

Έναν λογαριασμό που έχουμε δημιουργήσει στο παρελθόν , μπορούμε αν επιθυμούμε ανά πάσα στιγμή να τον τροποποιήσουμε , αλλάζοντας τόσο τις ρυθμίσεις του όσο και το όνομά του , την εικόνα του ακόμη και τον τύπο του .
Τα βήματα που πρέπει να ακολουθήσουμε για να τροποποιήσουμε έναν λογαριασμό χρήστη είναι τα ακόλουθα :

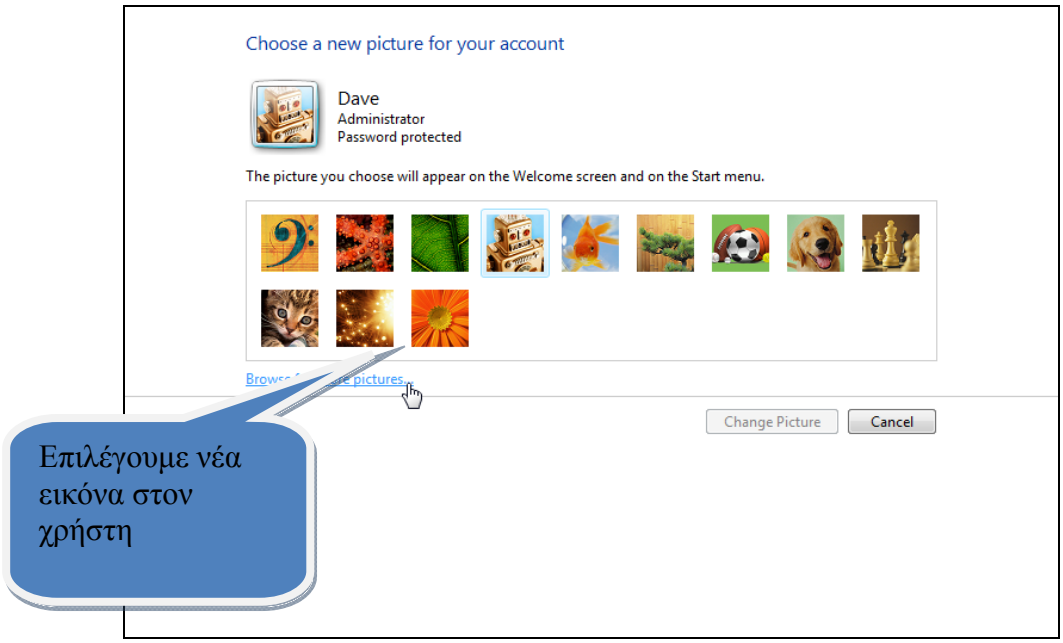
1. Κάνουμε κλικ στο στοιχείο **Αλλαγή ενός λογαριασμού (Change an account)** και στο πλαίσιο λίστας **Επιλογή μιας εργασίας (Pick a task).**
2. Κάνουμε κλικ στο λογαριασμό που θέλουμε να αλλάξουμε .
3. Επιλέγουμε το στοιχείο που θέλουμε να αλλάξουμε :

- Κάνουμε κλικ στην επιλογή **Αλλαγή του ονόματος (Change the name),** για να αλλάξουμε το όνομα που εμφανίζεται στην οθόνη υποδοχής για τον λογαριασμό.



Εικόνα 42 : Παράθυρο τροποποίησης ονόματος χρήστη .

- Κάνουμε κλικ στην επιλογή **Αλλαγή της εικόνας (Change the picture),** για να αλλάξουμε την εικόνα που χρησιμοποιούμε για την αναπαράσταση του λογαριασμού χρήστη. Μπορείτε να χρησιμοποιήσουμε οποιαδήποτε αρχείο εικόνας στον υπολογιστή για την εικόνα του χρήστη .

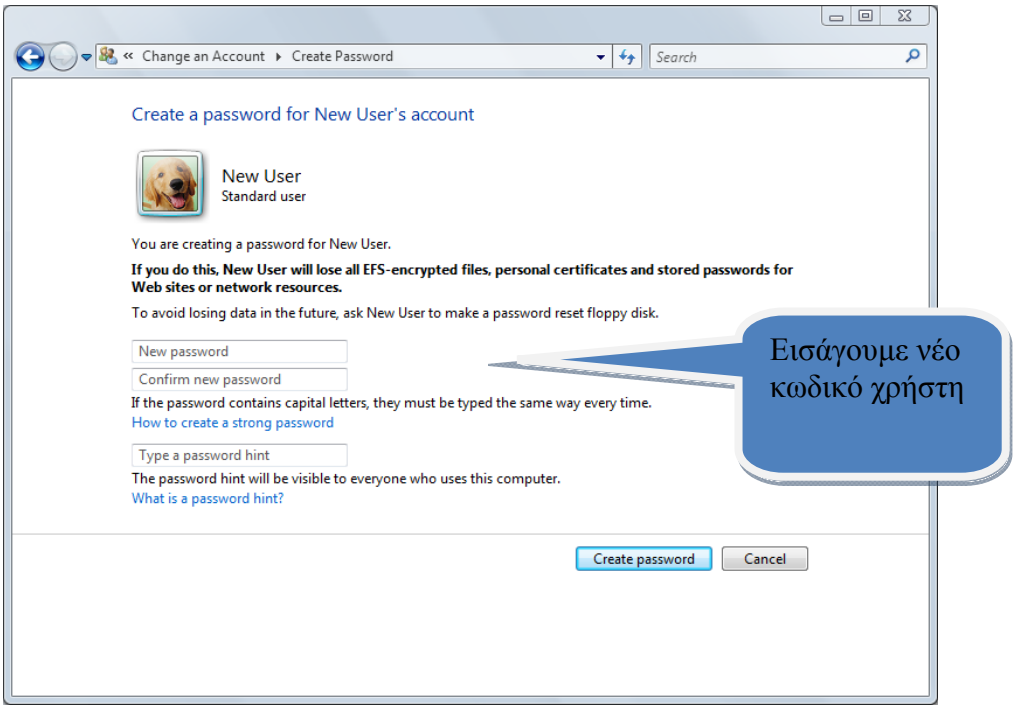


Εικόνα 43 :Παράθυρο αλλαγής εικόνας του χρήστη.

- Κάνουμε κλικ στην επιλογή **Αλλαγή του τύπου λογαριασμού (Change the account type),** για να αλλάξουμε τον τύπο λογαριασμού ώστε να αυξήσουμε ή να μειώσουμε τα δικαιώματα χρήστη στον υπολογιστή .

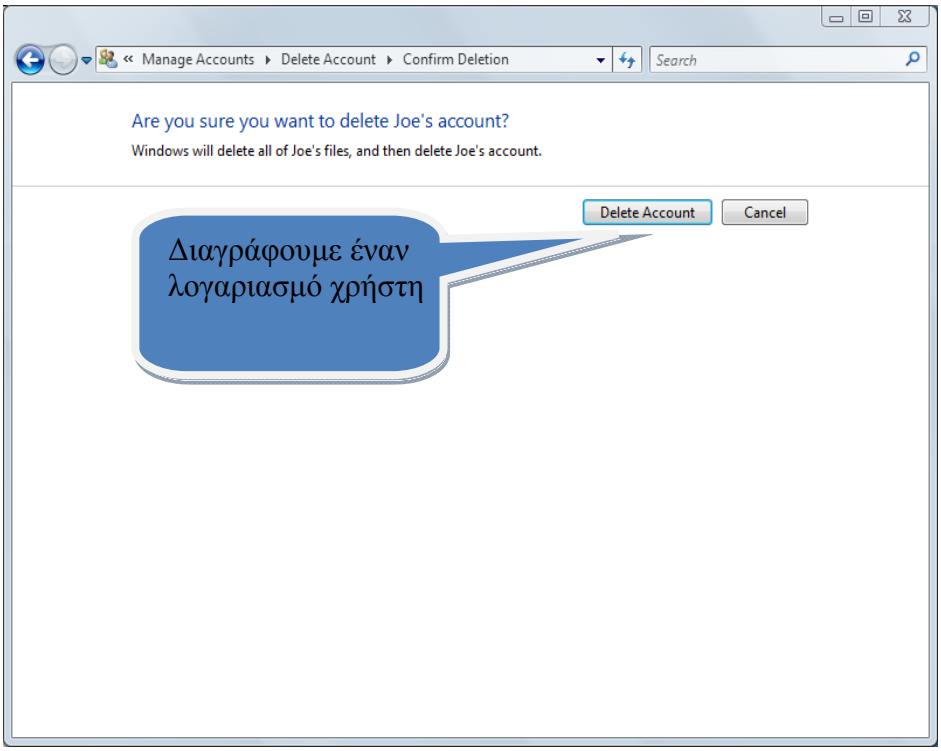
Εικόνα 44 : Παράθυρο αλλαγής του τύπου του λογαριασμού χρήστη .

- Κάνουμε κλικ στην επιλογή **Δημιουργία/αλλαγή του κωδικού πρόσβασης (Create/change the password),** για να δημιουργήσουμε ή να αλλάξουμε τον κωδικό πρόσβασης για τον χρήστη και να δημιουργήσουμε ή να αλλάξουμε την υπόδειξη κωδικού πρόσβασης.



Εικόνα 45 : Παράθυρο αλλαγής του κωδικού χρήστη.

- Κάνουμε κλικ στην επιλογή **Διαγραφή του λογαριασμού (Delete the account),** για να διαγράψουμε τον λογαριασμό χρήστη από τον υπολογιστή . Όταν διαγράψουμε το λογαριασμό , μας δίνεται η επιλογή να αποθηκεύσουμε τα αρχεία του χρήστη στον υπολογιστή .



Εικόνα 46 : Παράθυρο διαγραφής λογαριασμού χρήστη.

7.1.3 Πως λειτουργεί ο γονικός έλεγχος.

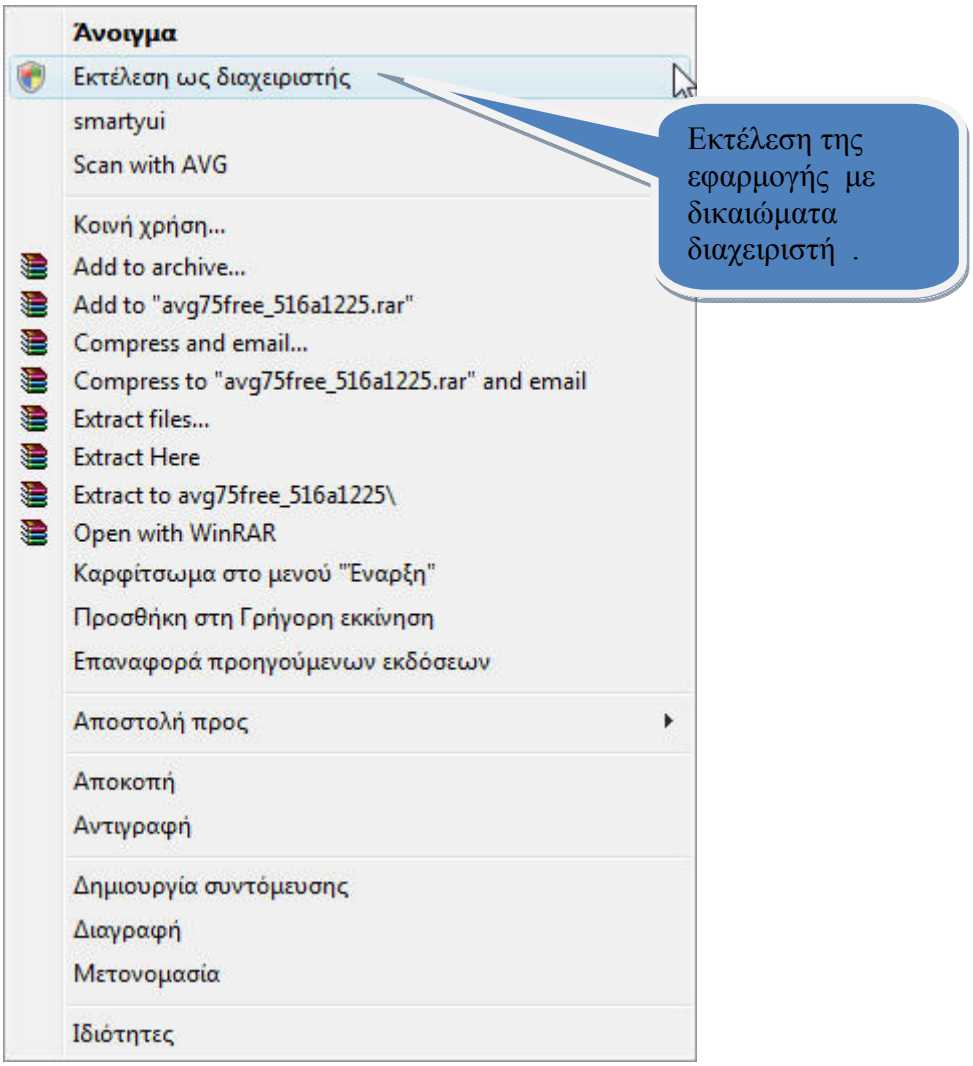
7.1.3.1 Δημιουργώντας εφαρμογές οι οποίες μπορούν να εκτελεστούν και από τον τυποποιημένο χρήστη

Γίνεται μια μεγάλη προσπάθεια να διευκολυνθεί η Microsoft αλλά και οι άλλοι προμηθευτές , να επανασχεδιάσουν τις εφαρμογές του περιορίζοντας τις απαιτήσεις (όσο αφορά τα δικαιώματα που απαιτούνται) του διαχειριστικού σημείου πρόσβασης του χρήστη. Κάποιες από αυτές τις επανασχεδιασμένες εφαρμογές κατάφεραν να το πετύχουν αυτό και από κει που αν δεν διέθεταν προνόμια διαχειριστή δεν εκτελόντουσαν , τώρα εκτελούνται και απαιτείται να είναι ο χρήστης διαχειριστής μόνο όταν είναι απολύτως απαραίτητο από την εφαρμογή .

Στο παρελθόν οι σχεδιαστές εκτελούσαν έναν έλεγχο πρόσβασης ,για να διασφαλίσουν ότι ο χρήστης είναι διαχειριστής , στην αρχική εκτέλεση της εφαρμογής. Πολλές από τις εφαρμογές αυτές , παρόλα αυτά δεν διέθεταν λειτουργίες οι οποίες πραγματικά να απαιτούσαν ο χρήστης να είναι ένας διαχειριστής.
Ορισμένα προγράμματα παρόλα αυτά πάντα θα απαιτούν ένα σημείο πρόσβασης διαχειριστή. Ένα τέτοιο παράδειγμα είναι ο διαμερισμός του λογισμικού του δίσκου .Τα προγράμματα τα οποία απαιτούν ο χρήστης να είναι διαχειριστής μπορούν να εκτελεστούν στα Windows Vista χρησιμοποιώντας το σημείο πλήρους πρόσβαση διαχειριστή οι ενέργειες όμως που ακολουθούνται όμως είναι : ο χρήστης πρώτα ειδοποιεί την αίτηση της εφαρμογής να προάγει τον χρήστη από διαχειριστή σε Admin Approval Mode σε έναν πλήρη διαχειριστή και στην συνέχεια ο χρήστης θα πρέπει να επιλέξει εάν θα αποδεχτεί ή θα αρνηθεί αυτήν την προαγωγή.

7.1.3.2 Ο Γονικός έλεγχος είναι ενεργός εξ ορισμού

Ο γονικός έλεγχος στα Windows Vista είναι ενεργός εξ ορισμού , σαν αποτέλεσμα οι χρήστες μπορεί να αντιμετωπίζουν κάποια προβλήματα συμβατότητας με διάφορες εφαρμογές , οι οποίες δεν έχουν ακόμη αναβαθμιστεί σχετικά με τον νέο μηχανισμό ασφαλείας των Windows Vista .
Εάν μια εφαρμογή απαιτεί ένα σημείο πρόσβασης διαχειριστή (αυτό καθορίζεται από το μήνυμα λάθους ¨απαγορεύεται η είσοδος ¨ που επιστρέφεται όταν προσπαθήσουμε να τρέξουμε μια εφαρμογή που δεν έχουμε πρόσβαση), μπορούμε να εκτελέσουμε την εφαρμογή αυτή χρησιμοποιώντας την επιλογή ¨ Εκτέλεση ως διαχειριστής (Run as administrator) ¨ η οποία βρίσκετε στο πλαίσιο μενού .



Εικόνα 47 : Παράθυρο πλαισίου μενού.

7.1.3.3 Όλοι οι ¨επόμενοι ¨ λογαριασμοί δημιουργούνται ως λογαριασμοί τυποποιημένων χρηστών .

Ταυτόχρονα ο λογαριασμός τυποποιημένου χρήστη και ο λογαριασμός διαχειριστή μπορούν να εκμεταλλευτούν από την ενισχυμένη ασφάλεια που προσφέρει ο UAC. Στις νέες εγκαταστάσεις , εξ ορισμού , ο πρώτος λογαριασμός χρήστη που δημιουργείται χαρακτηρίζεται ως λογαριασμός τυπικού διαχειριστή στο Admin Approval Mode . Όλοι οι δευτερεύοντες λογαριασμοί που δημιουργούνται στην συνέχεια χαρακτηρίζονται ως λογαριασμοί τυποποιημένων χρηστών .

7.1.3.4 Ο ενσωματωμένος λογαριασμός διαχειριστή χρήστη είναι ανενεργός εξ ορισμού σε κάθε νέα εγκατάσταση

Ο ενσωματωμένος λογαριασμός διαχειριστή είναι ανενεργός εξ ορισμού στα Windows Vista . Εάν τα Windows Vista , κατά την διάρκεια της αναβάθμισης από τα Windows XP ,καθορίσουν ότι ο ενσωματωμένος διαχειριστής είναι ο μόνος ενεργός τοπικός λογαριασμός διαχειριστή , τα Windows Vista αφήνουν ενεργό τον λογαριασμό τοποθετώντας τον μέσα στο πλαίσιο του Admin Approval Mode. Ο ενσωματωμένος λογαριασμός διαχειριστή , εξ ορισμού ακόμη ,δεν μπορεί να εισαχθεί στο σύστημα σε κατάσταση safe mode .

7.1.4 Γονικός έλεγχος Βήμα-Βήμα

Ο τρόπος λειτουργίας ενός τυποποιημένου χρήστη και ενός χρήστη διαχειριστή διαφέρει στο Admin Approval Mode όταν ο γονικός έλεγχος είναι ενεργός . Οι ακόλουθοι παράγραφοι , περιγράφουν με λεπτομέρειες τις διαφορές αυτές και εξηγούν τον τρόπο σχεδιασμού και λειτουργίας του γονικού ελέγχου .

7.1.4.1 Ενεργοποίηση & Απενεργοποίηση του Γονικού Ελέγχου UAC

Το UAC είναι ένα ιδιαίτερα χρήσιμο για τους νέους χρήστες πρόγραμμα που τους βοηθά να κατανοήσουν καλύτερα το τι συμβαίνει στο στον υπολογιστή τους . Έστω ότι επιθυμούμε να ενεργοποιήσουμε ή να απενεργοποιήσουμε τον μηχανισμό αυτόν, τα βήματα που πρέπει να ακολουθήσουμε είναι τα εξής :

1. Συνδεόμαστε στα Windows Vista ως ¨διαχειριστής¨.

2. Πηγαίνουμε στην **Έναρξη (Start)** και κατόπιν επιλέγουμε τον **Πίνακας Ελέγχου (Control Panel)**.

3. Στην συνέχεια διαλέγουμε την επιλογή **Λογαριασμοί χρηστών και οικογενειακή ασφάλεια (User Accounts and Family Safety)** , έπειτα πατάμε στην επιλογή **Λογαριασμοί χρήστη (User Accounts)** και έπειτα επιλέγουμε την **Ενεργοποίηση ή απενεργοποίηση ελέγχου λογαριασμού χρήστη(Turn User Account Control on or off)**.

Σε ορισμένες εκδόσεις των Windows Vista , το στοιχείο **Λογαριασμοί χρηστών και οικογενειακή ασφάλεια(User Accounts and Family Safety**) δεν εμφανίζεται . Στην θέση του , επιλέγουμε το στοιχείο **Λογαριασμοί χρήστη** (**User Accounts**) και στην συνέχεια ακολουθούμε τα ίδια βήματα με την πρώτη περίπτωση .

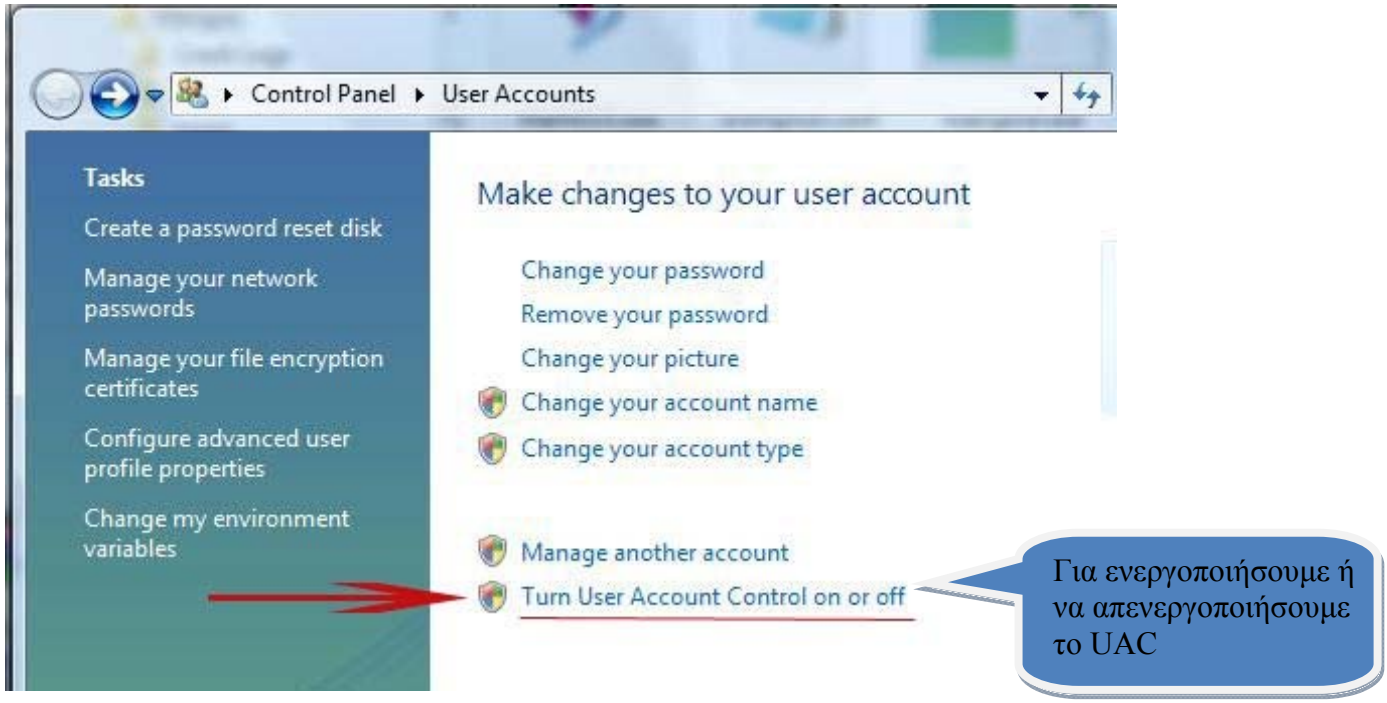
Εάν στην διάρκεια των βημάτων αυτών , μας ζητηθεί ο κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση ,πληκτρολογούμε τον κωδικό που έχουμε ρυθμίσει εξ αρχής και κάνουμε κλικ στην επιλογή **Συνέχεια (continue)** .

4. Σαν επόμενο βήμα επιλέγουμε το πλαίσιο ελέγχου **Χρησιμοποιούμε τον έλεγχο λογαριασμού χρήστη (UAC) για την ασφάλεια του υπολογιστή σας (User Account Control (UAC) to help protect your computer)** .

5. Κάνουμε κλικ στο κουμπί **OK** .

6. Όταν μας ζητηθεί , ξεκινάμε πάλι τον υπολογιστή .

Αφού ολοκληρώσουμε τα παραπάνω βήματα , εμφανίζεται το παράθυρο Έλεγχος λογαριασμού χρήστη (User Account Control) , έχουμε ολοκληρώσει την διαδικασία της ενεργοποίησης του UAC.

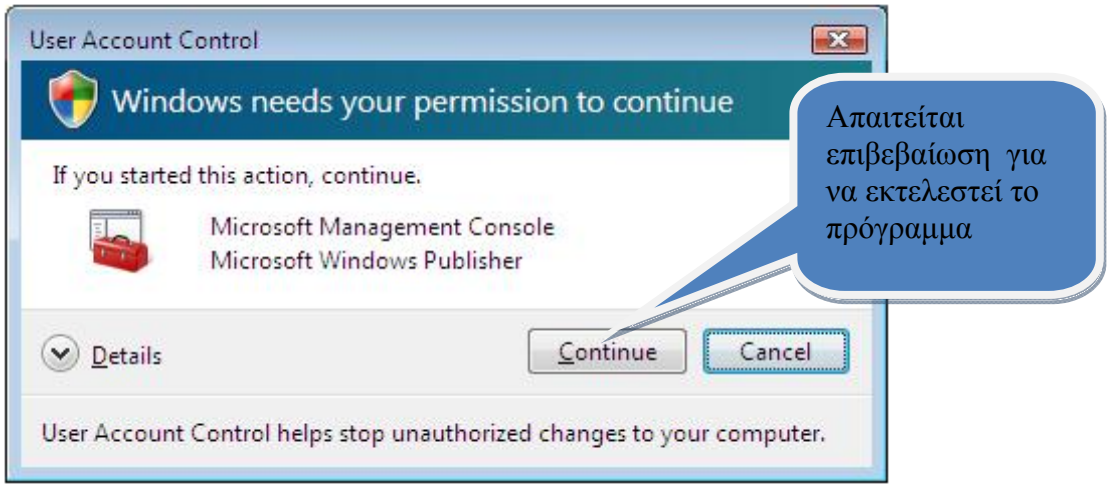


Εικόνα 48 : Κεντρικό παράθυρο Γονικού Ελέγχου.

7.1.4.2 Παροχή συγκατάθεσης

Με ενεργό τον UAC , τα Windows Vista παρέχουν συγκατάθεση και παρέχουν πιστοποιητικά για έναν έγκυρο λογαριασμό διαχειριστή πριν ακόμη τεθεί σε λειτουργία ένα πρόγραμμα ή μια εργασία τα οποία περιέχουν πλήρους διαχειριστή σημείο πρόσβασης . Αυτός ο τρόπος βοηθάει εν μέρη να προληφθεί η αθόρυβη εγκατάσταση των malware .
Η παροχή συγκατάθεσης παρουσιάζεται όταν ένας διαχειριστής επιχειρεί να εκτελέσει μια εργασία η οποία απαιτεί πλήρους διαχειριστή χρήστη σημείο πρόσβασης , αυτή η προεπιλογή είναι για τον διαχειριστή διαμορφώσιμη μέσω της τοπικής πολιτικής ασφάλειας και των πολιτικών του γκρουπ . Στην παρακάτω εικόνα παρουσιάζεται η παροχή συγκατάθεσης του UAC.

(Προκειμένου να ολοκληρωθεί ή να εκτελεστεί μιας λειτουργίας απαιτείται η άδεια ή το password από τον administrator , το UAC μας ενημερώνει με ένα από τα παρακάτω μηνύματα).



Εικόνα 49 : Παράθυρο ειδοποίησης.

Το ακόλουθο παράδειγμα μας δείχνει πως σε έναν διαχειριστή ,στο πλαίσιο του Admin Approval Mode , του ζητείται παροχή συγκατάθεσης όταν προσπαθεί να εκτελέσει μια εργασία που απαιτεί προνόμια διαχειριστή .

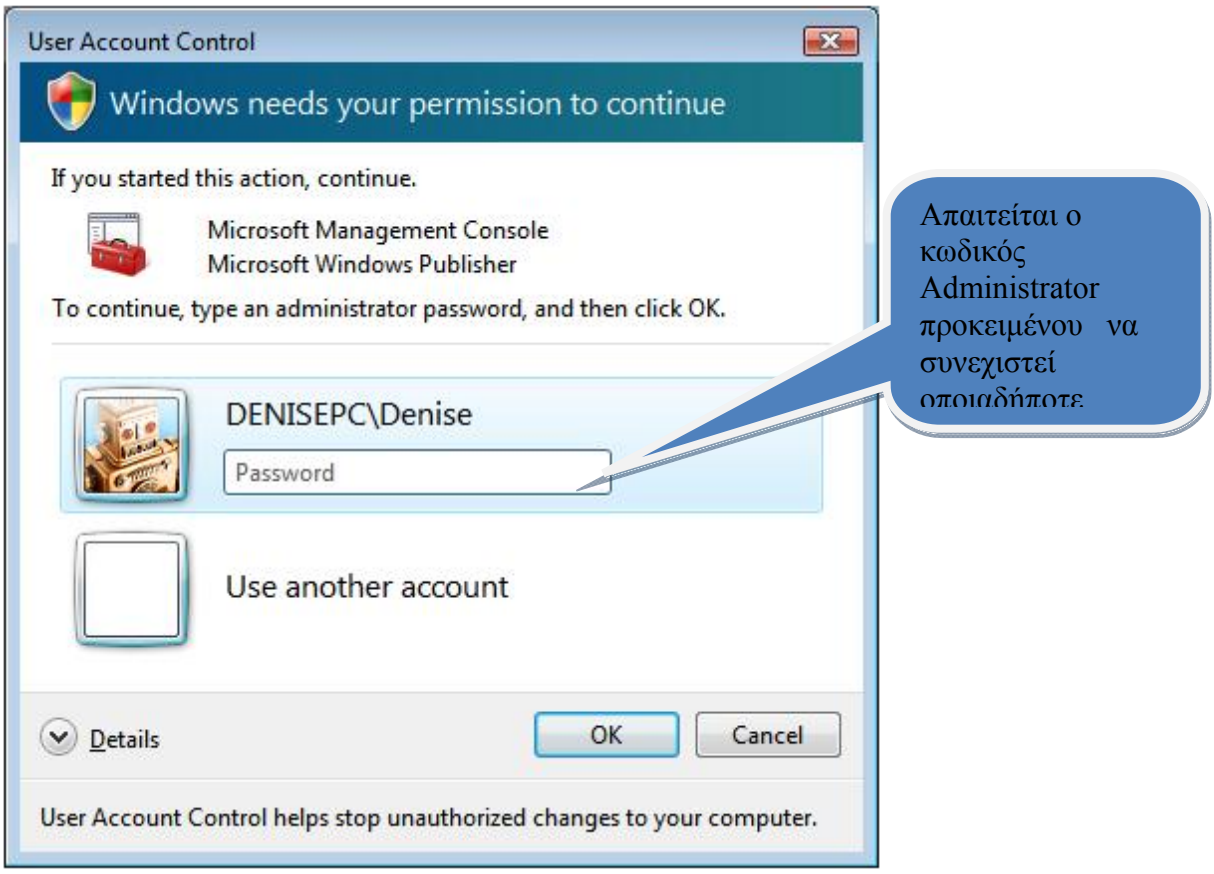
Για να μας εμφανιστεί το πλαίσιο της παροχής συγκατάθεσης :

1. Πρέπει να κάνουμε εισαγωγή σε έναν λογαριασμό διαχειριστή στα Windows Vista , σε Admin Approval Mode.
2. Στην συνέχεια πρέπει να πατήσουμε κλικ στο κουμπί της **έναρξης** , και **μετά δεξί κλικ** πάνω στο εικονίδιο του υπολογιστή μας και από το μενού που θα εμφανιστεί πρέπει να επιλέξουμε την επιλογή **Διαχείριση** .
3. Στο πλαίσιο του UAC που θα μας εμφανιστεί (όμοιο με το παραπάνω σχήμα) , πατάμε το κουμπί **συνέχεια** για να ολοκληρωθεί η παροχή της συγκατάθεσης .

7.1.4.3 Παροχή πιστοποιητικού

Η παροχή πιστοποιητικού παρουσιάζεται όταν ένας τυποποιημένος χρήστης επιχειρεί να εκτελέσει μια εργασία η οποία απαιτεί διαχειριστικό σημείο πρόσβασης του χρήστη . Ομοίως και σε αυτήν την περίπτωση όπως και πριν με την συγκατάθεση ,η προεπιλογή είναι για τον διαχειριστή διαμορφώσιμη μέσω της τοπικής πολιτικής ασφάλειας και των πολιτικών του γκρουπ.

Οι διαχειριστές μπορούν επίσης να απαιτήσουν να τους δοθεί πιστοποιητικό μέσω των ρυθμίσεων του UAC . Η ακόλουθη εικόνα είναι ένα παράδειγμα παροχής πιστοποιητικού του γονικού ελέγχου .



Εικόνα 50 :Παράθυρο ειδοποίησης .

Το παραπάνω παράδειγμα μας δείχνει πως σε έναν τυποποιημένος χρήστης ,στο πλαίσιο του Admin Approval Mode , του ζητείται παροχή πιστοποιητικού όταν προσπαθεί να εκτελέσει μια εργασία που απαιτεί προνόμια διαχειριστή .

Για να μας εμφανιστεί το πλαίσιο της παροχής πιστοποιητικού :

1. Πρέπει να κάνουμε εισαγωγή σε έναν λογαριασμό τυποποιημένου χρήστη στα Windows Vista , σε Admin Approval Mode.

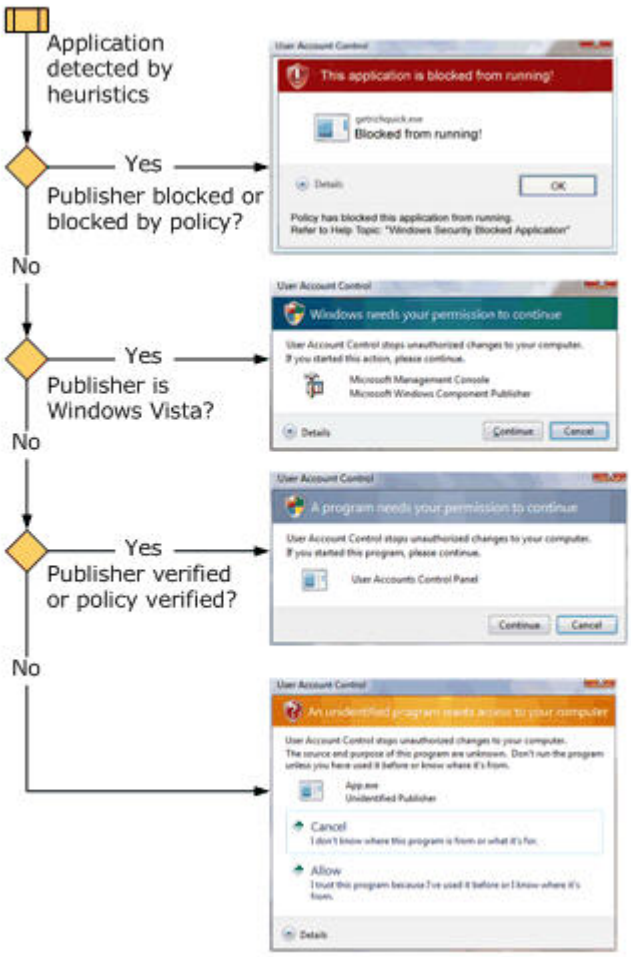
2. Στην συνέχεια πρέπει να πατήσουμε κλικ στο κουμπί της **έναρξης** , και **μετά δεξί κλικ** πάνω στο **εικονίδιο του υπολογιστή μας** και από το μενού που θα εμφανιστεί πρέπει να επιλέξουμε την επιλογή **Διαχείριση** .

3. Στο πλαίσιο διαλόγου του UAC , πατάμε **το username** του κατάλληλου διαχειριστή , στην συνέχεια πρέπει να εισάγουμε το **password** του συγκεκριμένου λογαριασμού του χρήστη και μετά πρέπει να κάνουμε κλικ στο **κουμπί αποδοχής (OK).**

7.1.4.4 Γνωστά πλαίσια υπαγόρευσης διαφόρων ενεργειών

Τα διάφορα πλαίσια του UAC που εμφανίζονται κατά την διάρκεια των προσπαθειών μας να εκτελέσουμε διάφορες ενέργειες , είναι χρωμο-κωδικοποιημένα , δηλαδή από το χρώμα τους μπορούμε να ξεκαθαρίσουμε εάν είναι πλαίσιο παροχής συγκατάθεσης , ή πιστοποιητικού κ.α.

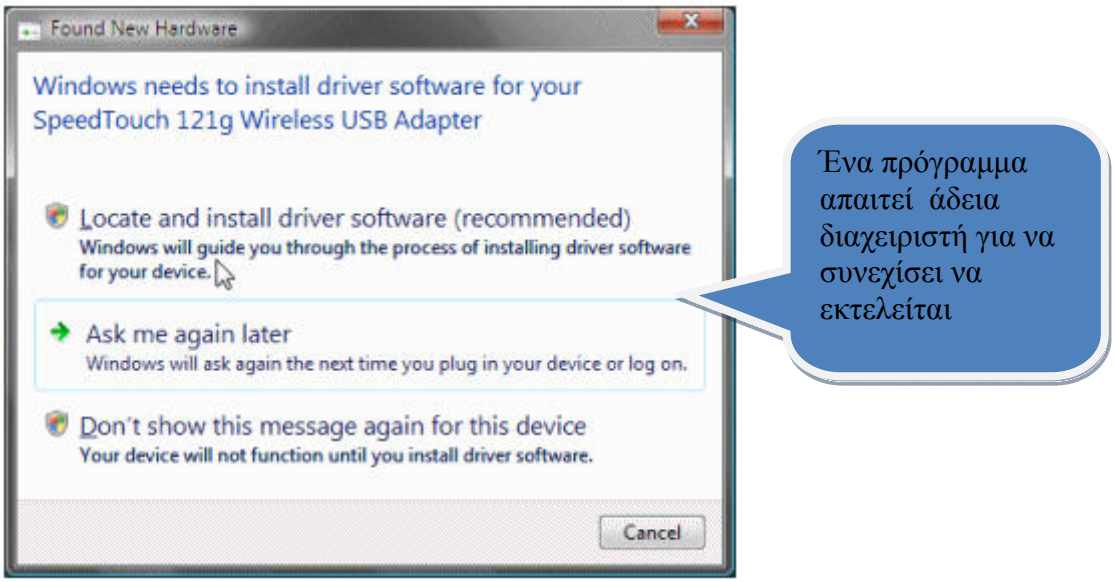
Είναι ενεργοποιημένα έτσι ώστε να αναγνωρίζουμε άμεσα έναν πιθανό κίνδυνο ασφάλειας μιας εφαρμογής .
Όταν μια εφαρμογή επιχειρεί να τρέξει μέσω ενός πλήρους σημείου πρόσβασης διαχειριστή, αρχικά τα Windows Vista αναλύουν την εκτελέσιμη εφαρμογή προκειμένου έτσι να καθορίσουν τον εκδότη αυτών που εμφανίζονται . Οι εφαρμογές είναι αρχικά μοιρασμένες σε τρείς κατηγορίες , με βάση τον εκδότη της εκτέλεσης τους : α) από τα Windows Vista, β) από εκδότης που ελέγχεται (εγγεγραμμένος), γ) από εκδότη που δεν ελέγχεται (μη εγγεγραμμένο) .
Το ακόλουθο διάγραμμα παρουσιάζει πως τα Windows Vista καθορίζουν πιο χρώμα πλαισίου υπαγόρευσης θα εμφανίζεται στον εκάστοτε χρήστη .



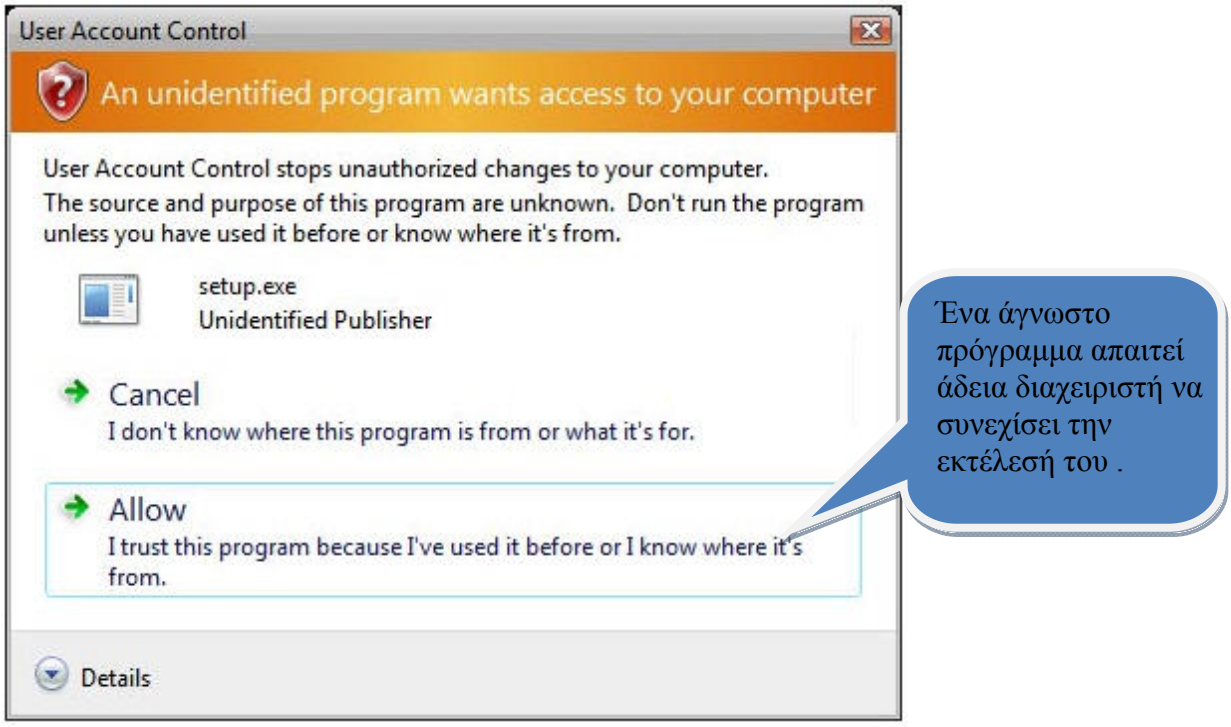
Εικόνα 51 : Παράθυρα ειδοποιήσεων .

- **Κόκκινο background και κόκκινο εικονίδιο ασπίδας** : Η εφαρμογή προέρχεται από έναν μπλοκαρισμένο εκδότη ή μπλοκάρεται από το Group Policy .
- **Μπλε πράσινο background** : Η εφαρμογή είναι μια εφαρμογή των Window Vista που απαιτεί προνόμια διαχωριστή , όπως πχ ο πίνακας ελέγχου .
- **Γκρίζο background και χρυσό εικονίδιο ασπίδας** : Η εφαρμογή είναι επικυρωμένη, υπογεγραμμένη και έχει χαρακτηριστεί έμπιστη εφαρμογή από το τοπικό υπολογιστή .
- **Κίτρινο background και κόκκινη ασπίδα** : Η εφαρμογή είναι είτε μη υπογεγραμμένη είτε υπογεγραμμένη αλλά δεν έχει χαρακτηριστεί ως έμπιστη ακόμη από τον τοπικό υπολογιστή .

Ο χρωματοκώδικας των πλαισίων αυτών είναι παράλληλος με αυτόν τον χρωματοκώδικα των πλαισίων διαλόγων του Microsoft Internet Explorer .



Εικόνα 52 : Παράθυρο ειδοποίησης .



Εικόνα 53 : Παράθυρο ειδοποίησης .

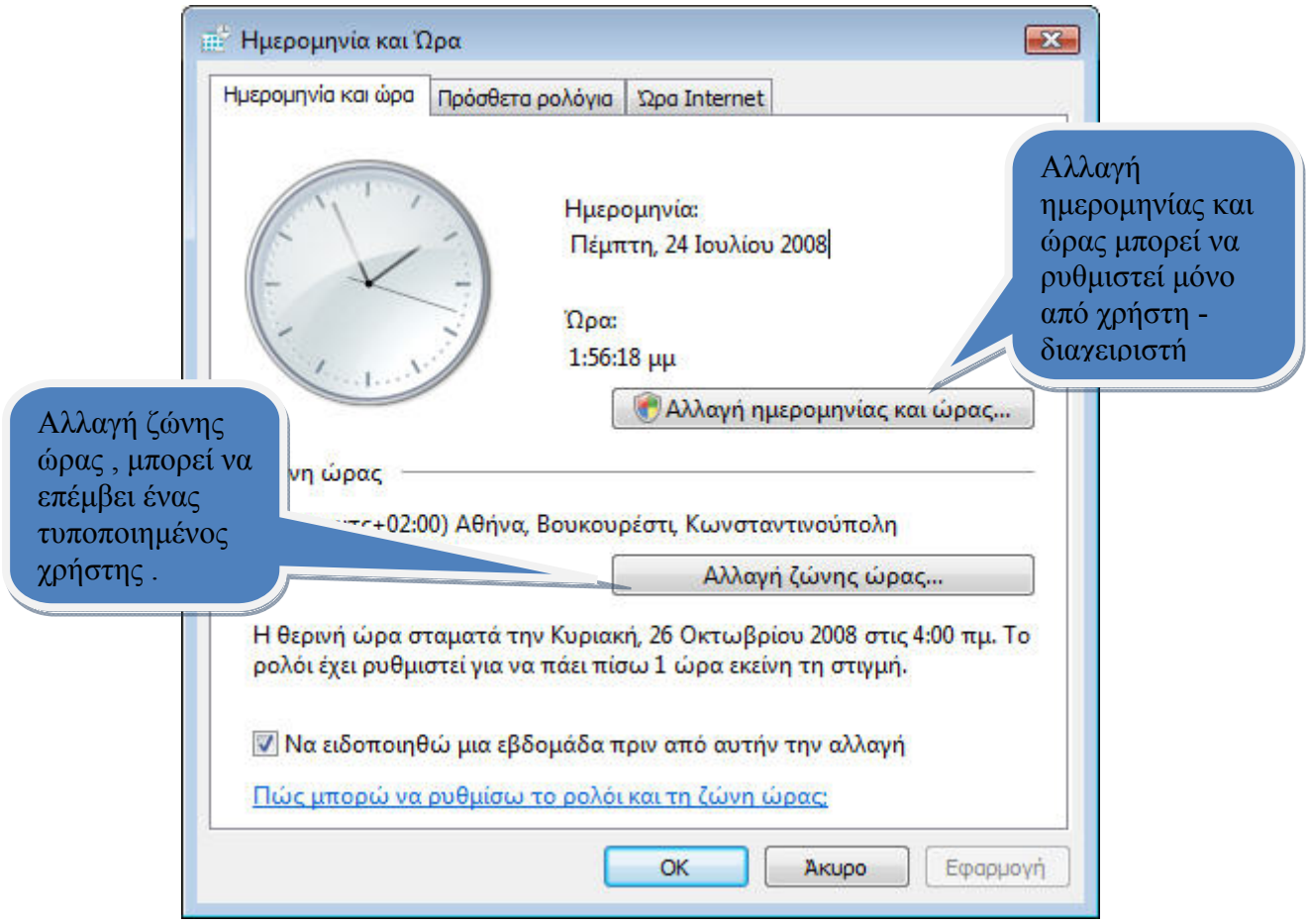
Εικόνα 54 : Παράθυρο ειδοποίησης .

Αυτά τα μηνύματα ασφαλείας των Windows μας εμφανίζονται καθώς εκτελούμε εργασίες ως βασικός χρήστης και ο μηχανισμός User Account Control είναι ενεργοποιημένος . Θα μπορούσαμε να αποφύγουμε την εμφάνιση τους ή να τις προσπεράσουμε ένα μας εμφανιστούν με τους εξής τρόπους :

- Είτε με το να συνδεόμαστε στα Windows Vista ως διαχειριστής ,
- είτε πετώντας δεξί κλικ σε ένα πρόγραμμα ή σε μια εργασία που εκτελούμε και κατόπιν πατώντας την εντολή Εκτέλεση ως διαχειριστής (Run as administrator).

7.1.4.5 Εικονίδιο ασπίδας

Μερικά από τα πλαίσια ελέγχου των Windows Vista , όπως για παράδειγμα αυτό του **Ημερομηνία και Ώρα** πίνακα ελέγχου , περιέχει ένα συνδυασμό από λειτουργίες τόσο τυποποιημένου χρήστη όσο και διαχειριστή . Οι τυποποιημένοι χρήστες , έχουν πρόσβαση στο να δουν το ρολόι και να αλλάξουν την ώρα της ζώνης , από την άλλη ένα πλήρους διαχειριστικό σημείο πρόσβασης απαιτείται να αλλάζει την ώρα του συστήματος .
Η παρακάτω εικόνα είναι το πλαίσιο του πίνακα ελέγχου της Ημερομηνίας και Ώρας .

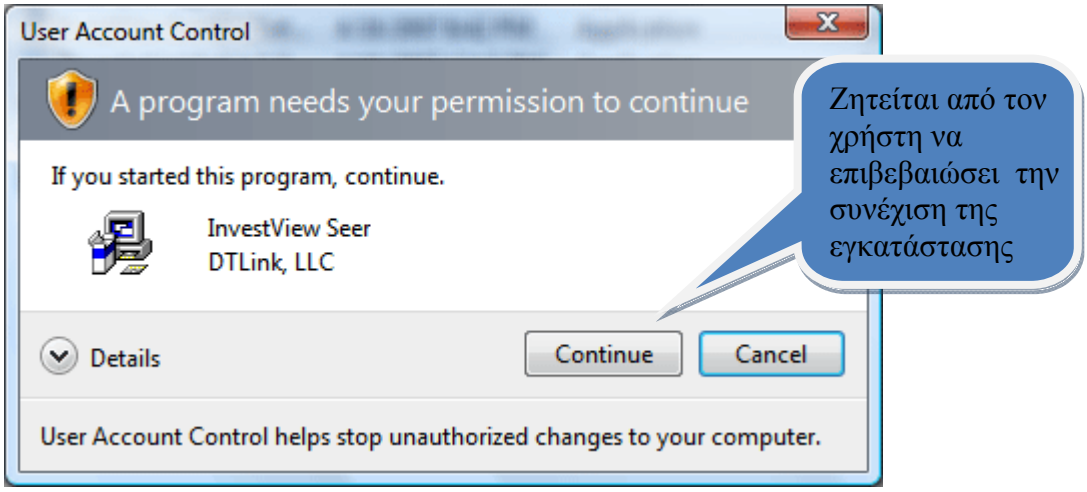


Εικόνα 55: Παράθυρο πίνακα ελέγχου Ημερομηνίας και Ώρας .

Όταν ένα χρήστης θέλει να ρυθμίσει την ώρα , πρέπει να πατήσει κλικ πάνω στο κουμπί **Αλλαγή ημερομηνίας κα ώρας** , το οποίο έχει την ασπίδα των Windows δίπλα του . Η ασπίδα αυτή υποδηλώνει ότι χρειάζεται να χρησιμοποιηθεί σημείο πρόσβασης πλήρους διαχειριστή και η οποία ενέργεια για να συνεχιστεί θα της ζητηθεί να περάσει από τον έλεγχο του UAC.

7.1.4.6 Εγκατάσταση και εκτέλεση προγράμματος με ενεργό τον Γονικό έλεγχο

Για την εγκατάσταση μερικών εφαρμογών στο σύστημα , απαιτείται σημείο πρόσβασης διαχειριστή , ένας μηχανισμός είναι τοποθετημένος μαζί με το λειτουργικό σύστημα των Windows Vista και ο οποίος αυτόματα ανιχνεύει την έναρξη μιας εγκατάστασης .
Μόλις ανιχνευτεί η εγκατάσταση αυτή της εφαρμογής , ο UAC εμφανίζει ένα πλαίσιο προτροπής προς τον χρήστη και τον προτρέπει να επικυρώσει της εγκατάσταση της διαδικασίας αυτής .Στην συνέχεια της εγκατάστασης , δεν θα απαιτηθεί από την εφαρμογή του χρήστη να παρέχει οποιοδήποτε πιστοποιητικό , εκτός και αν είναι εφαρμογή είναι διοικητική .



Εικόνα 56 : Παράθυρο επικύρωση εγκατάστασης .

7.1.4.7 Αλλαγή μεταξύ της παροχής πιστοποιητικού και της παροχής συγκατάθεσης

Οι χρήστες στα Windows Vista μπορούν ελέγχουν τι είδους προτροπές (πιστοποιητικών , συγκατάθεσης ή άλλα) θα απαιτούνται για τον εκάστοτε χρήστη . Αυτό επιτυγχάνεται μέσω καθορισμού νέων πολιτικών ασφάλειας οι οποίοι παρουσιάζονται στα Windows Vista .

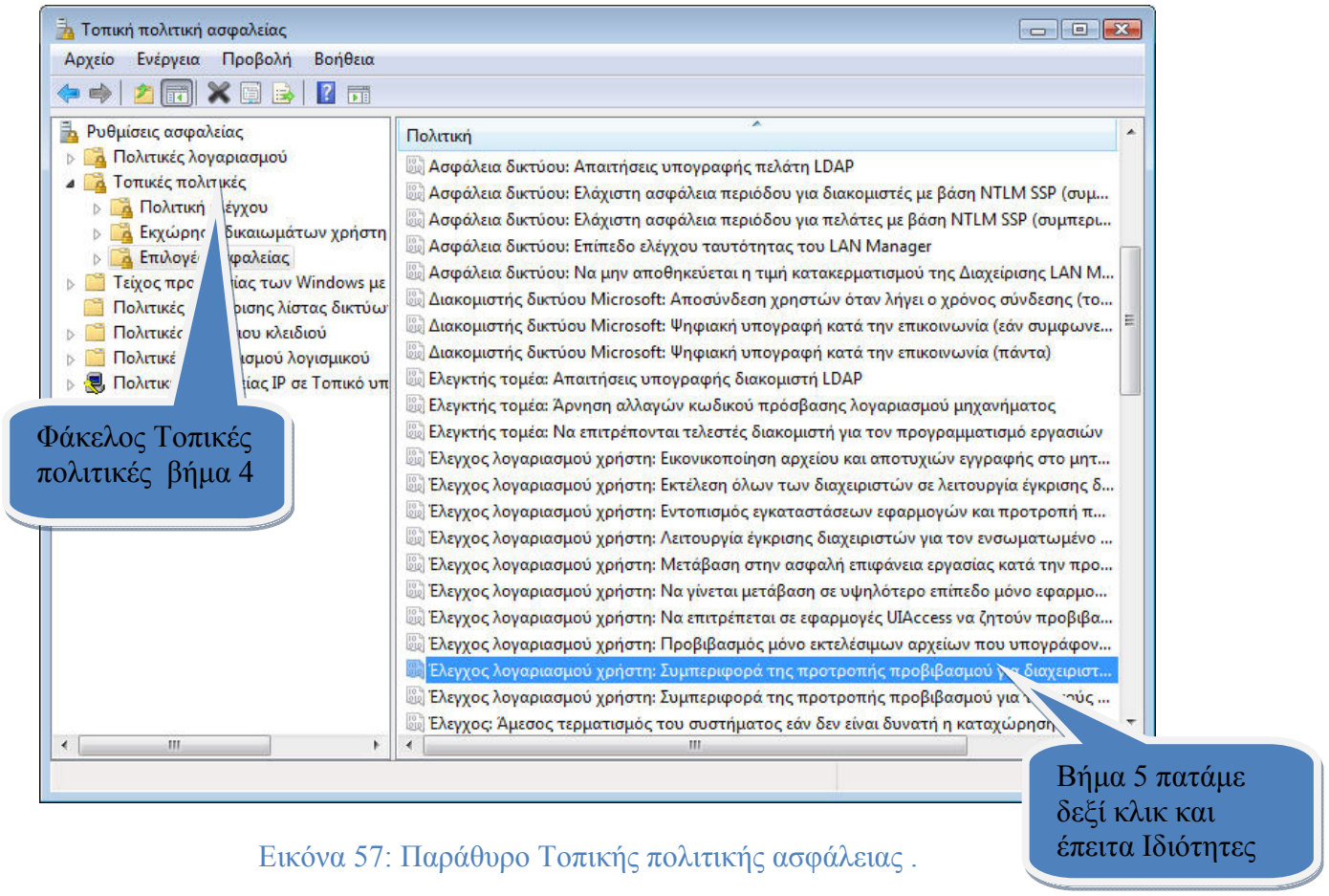
Αυτές οι ρυθμίσεις βρίσκονται στο **Security Policy Manager Microsoft Management Console (MMC)** , το οποίο μπορούμε να βρούμε ακολουθώντας το ακόλουθο μονοπάτι : **Local Security Settings -> Local Policies-> Security Options .**

Μπορούμε να ρυθμίσουμε την συμπεριφοράς της προτροπής προβιβασμού , χωριστά για τους διαχειριστές και χωριστά για τους τυποποιημένους χρήστες. Ακολουθεί λεπτομερειακή περιγραφή της συμπεριφοράς της προτροπής προβιβασμού του διαχειριστή του UAC στο πλαίσιο του Admin Approval Mode.
Η ενέργεια αυτή ναι μεν μπορεί να πραγματοποιηθεί τόσο από έναν τυποποιημένο χρήστη όσο και από έναν διαχειριστή αλλά οι ρυθμίσεις έχουν να κάνουν με τον τρόπο λειτουργίας του διαχειριστή .

7.1.4.8 Ρύθμιση της UAC συμπεριφοράς της προτροπής προβιβασμού για χρήστη διαχειριστή .

1. Είσοδος σε έναν υπολογιστή με Windows Vista , με χρήση λογαριασμού διαχειριστή .
2. Πατάμε στο κουμπί **Έναρξη** , στην συνέχεια στην Έναρξη αναζήτησης πατάμε την εντολή **secpol.msc**, και τέλος πατάμε **OK** .

3. Στο παράθυρο διαλόγου του UAC που εμφανίζεται για την **Microsoft Management Console** , πατάμε **Συνέχεια** .
4. Στο παράθυρο **Τοπική πολιτική ασφάλειας** που εμφανίζεται , στο μενού **Ρυθμίσεις ασφάλειας** πατάμε στον φάκελο με την ονομασία **Τοπικές πολιτικές** και τέλος πατάμε στο **Επιλογές ασφάλειας** .
5. Τέλος πατάμε πάνω **στο UAC : Συμπεριφορά της προτροπής προβιβασμού για διαχειριστές** δεξί κλικ και πατάμε στο **Ιδιότητες**

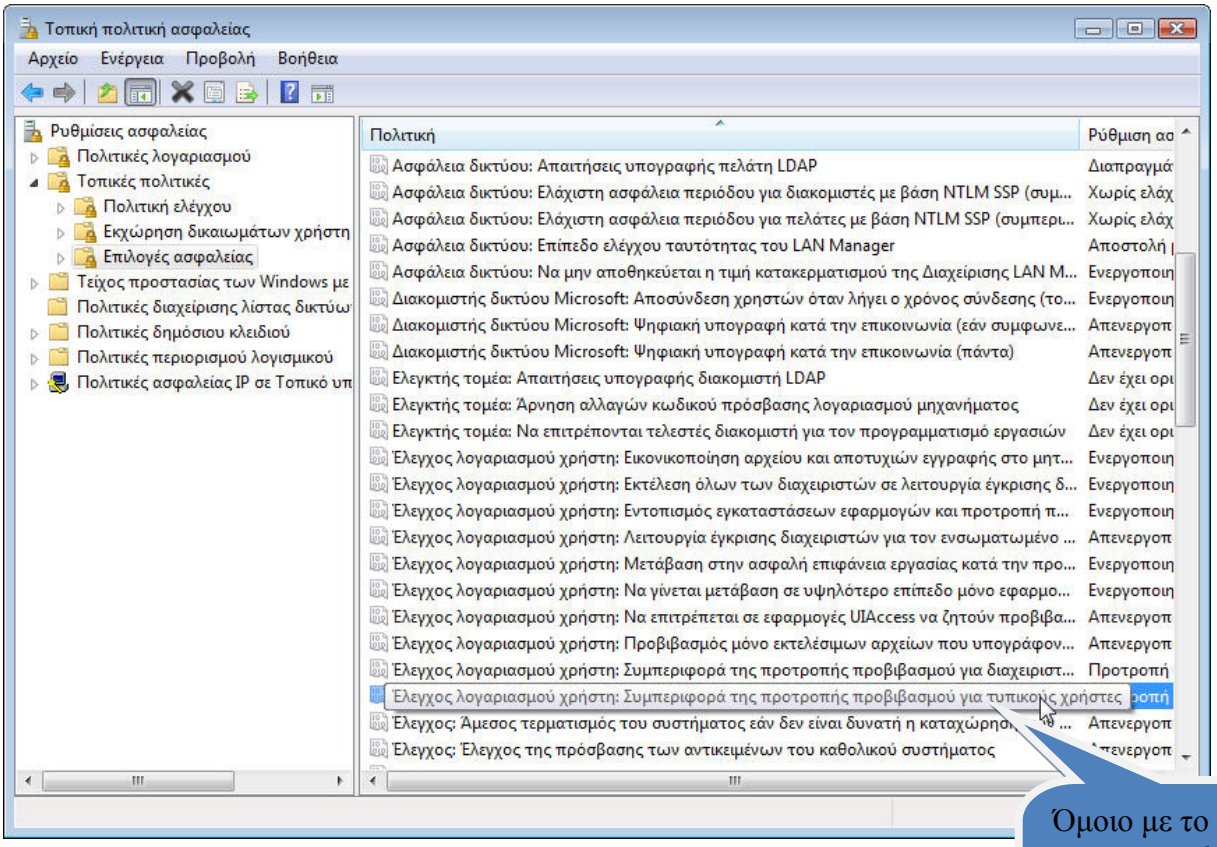


Εικόνα 57: Παράθυρο Τοπικής πολιτικής ασφάλειας .

7.1.4.9 Ρύθμιση της UAC συμπεριφοράς της προτροπής προβιβασμού για τυποποιημένο χρήστη .

1. Είσοδος σε έναν υπολογιστή με Windows Vista , με χρήση λογαριασμού διαχειριστή .
2. Πατάμε στο κουμπί **Έναρξη** , στην συνέχεια στην Έναρξη αναζήτησης πατάμε την εντολή **secpol.msc**, και τέλος πατάμε **OK** .
3. Στο παράθυρο διαλόγου του UAC που εμφανίζεται για την **Microsoft Management Console** , πατάμε **Συνέχεια** .

4. Στο παράθυρο **Τοπική πολιτική ασφάλειας** που εμφανίζεται , στο μενού **Ρυθμίσεις ασφάλειας** πατάμε στον φάκελο με την ονομασία **Τοπικές πολιτικές** και τέλος πατάμε στο **Επιλογές ασφάλειας** .
5. Τέλος πατάμε πάνω **στο UAC : Συμπεριφορά της προτροπής προβιβασμού για τυποποιημένο χρήστη** δεξί κλικ και πατάμε στο **Ιδιότητες .**



Εικόνα 58 : Παράθυρο Τοπικής πολιτικής ασφάλειας .

Όμοιο με το Βήμα 5 της προηγούμενης περίπτωσης μόνο τώρα που είναι για απλό χρήστη

Ο ακόλουθος πίνακας περιγράφει τις ρυθμίσεις της συμπεριφορά της προτροπής προβιβασμού τόσο για τον διαχειριστή όσο και για κάποιον τυποποιημένο χρήστη .

Πίνακας 4: Πολιτική συμπεριφοράς της προτροπής προβιβασμού

ΠΟΛΙΤΙΚΗ ΣΥΜΠΕΡΙΦΟΡΑΣ ΤΗΣ ΠΡΟΤΡΟΠΗΣ ΠΡΟΒΙΒΑΣΜΟΥ		
Ρυθμίσεις	**Περιγραφή**	**Προεπιλεγμένη τιμή**
Συμπεριφορά προτροπής προβιβασμού για Διαχειριστή	Υπάρχουν τρείς πιθανές τιμές : 1. Χωρίς προτροπή – Η ενέργεια εκτελείται αυτόματα και αθόρυβα 2. Προτροπή για παροχή συγκατάθεσης – ο UAC ζητάει να γίνει συγκατάθεση προτού συνεχιστεί η εκτέλεση της ενέργειας. 3. Προτροπή για παροχή πιστοποιητικού – ο UAC απαιτεί να εισαχθούν έγκυρα πιστοποιητικά διαχειριστή προτού να εκτελεστεί η εργασία. Η πολιτική αυτή επιδρά μόνο όταν ο UAC είναι ενεργός .	Προτροπή για συγκατάθεση
Συμπεριφορά προτροπής προβιβασμού για Τυποποιημένο χρήστη	Υπάρχουν δύο πιθανές τιμές : 1. Χωρίς προτροπή – Δεν παρουσιάζεται προτροπή προβιβασμού , και ο χρήστης δεν μπορεί να εκτελέσει διοικητικές εργασίες χωρίς να ¨τρέχει¨ σαν διαχειριστής ή χωρίς να εισάγεται στο σύστημα μέσω ενός λογαριασμού	Προτροπή για πιστοποιητικό

	διαχειριστή. 2. Προτροπή για πιστοποιητικό – ο UAC απαιτεί να εισαχθούν έγκυρα πιστοποιητικά διαχειριστή προτού να εκτελεστεί η εργασία	

Οποιαδήποτε αλλαγή και αν επιφέρουμε στις ρυθμίσεις της συμπεριφοράς της προτροπής προβιβασμού , θα πρέπει να γίνει με πάρα πολύ μεγάλη προσοχή . Αυτή η πολιτική είναι διαμορφώσιμη τόσο για τον διαχειριστή όσο και για τον τυποποιημένο χρήστη . Οι ακόλουθες γενικές οδηγίες καθοδήγησης , μπορούν να μας βοηθήσουν να κατανοήσουμε πώς ρυθμίζεται η συμπεριφορά προτροπής για το δικό μας προσωπικό περιβάλλον .

7.1.4.10 Διαχειριστές στο πλαίσιο του Admin Approval Mode

Η επιλογή **προτροπή συγκατάθεση** , συστήνεται σχεδόν στα περισσότερα περιβάλλοντα εργασίας . Τα πιο ασφαλή περιβάλλοντα εργασίας θα πρέπει να χρησιμοποιούν την επιλογή **προτροπή πιστοποιητικού.**
Η Microsoft μας προτρέπει ισχυρά να μην χρησιμοποιούμε την επιλογή **χωρίς προτροπή.** Με το να θέτουμε εκτός λειτουργίας την συμπεριφορά της προτροπής συμβιβασμού του UAC , αφαιρούμε από τον χρήστη την ικανότητα να εγκρίνει μια εφαρμογή προτού αυτή εκτελεστεί . Σαν αποτέλεσμα , οποιαδήποτε εφαρμογή , συμπεριλαμβανομένων των malware , μπορεί να προβιβάζεται αθόρυβα και να χρησιμοποιεί διοικητικά σημεία πρόσβασης , χωρίς την έγκριση του χρήστη .

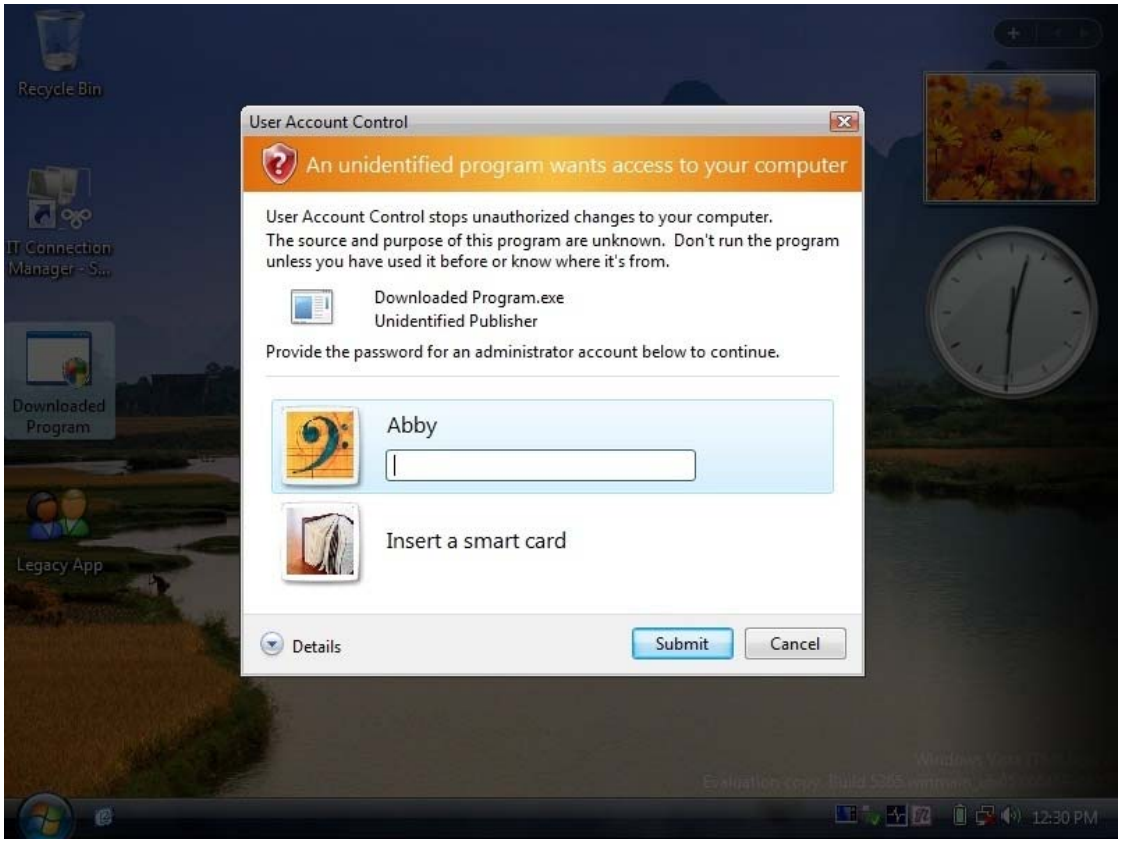
7.1.4.11 Τυποποιημένοι χρήστες

Η Microsoft προτείνει ότι οι τυποποιημένη χρήστες θα πρέπει να προτρέπονται για πιστοποιητικά διαχειριστών . Όταν η επιλογή ¨**χωρίς προτροπή**¨ είναι ενεργοποιημένη , οι τυποποιημένοι χρήστες δεν είναι σε θέση να εκτελέσουν οποιαδήποτε διοικητική εργασία χωρίς να ¨τρέχουν ¨ σαν διαχειριστές , είτε χωρίς να κάνουν log in μέσα σε έναν διοικητικό λογαριασμό , ή να είναι μέλη ενός γκρουπ διαχειριστών

7.1.4.12 Ασφαλής Επιφάνεια εργασίας .

Η προτροπή συγκατάθεσης και πιστοποιητικών εμφανίζονται στην ασφαλή λειτουργία εξ ορισμού στα Windows Vista . Μόνο οι διεργασίες των Windows έχουν πρόσβαση στην ασφαλή λειτουργία . Εκτός από τις συστάσεις , στους διαχειριστές και τους τυποποιημένους χρήστες , η Microsoft επίσης προτείνει ο UAC να μετατρέπει τις ρυθμίσεις σε μοντέλο ασφαλούς λειτουργίας όταν προτρέπεται για προβιβασμό, κρατώντας έτσι εφικτό ένα υψηλότερο επίπεδο ασφάλειας .

Όταν μια εργασία η οποία εκτελείται απαιτήσει μια προτροπή , η **αλληλεπιδραστική επιφάνεια εργασίας** ή αλλιώς η επιφάνεια εργασίας του χρήστη , μετατρέπεται σε ασφαλή επιφάνεια εργασίας . Η ασφαλή επιφάνεια , δίνει έναν συνδυασμό μιας μαυρισμένης επιφάνειας εργασίας του χρήστη και εμφανίζει πιο τονισμένα με έντονα χρώματα την προτροπή προβιβασμού (όπως η εικόνα παρακάτω). Όταν ο χρήστης πατήσει **Συνέχεια (Continue)** ή **Άκυρο(Cancel)** η επιφάνεια εργασίας μετατρέπεται πάλι στην αρχικής της μορφή .



Εικόνα 59: Παράθυρο ασφαλής επιφάνειας εργασίας .

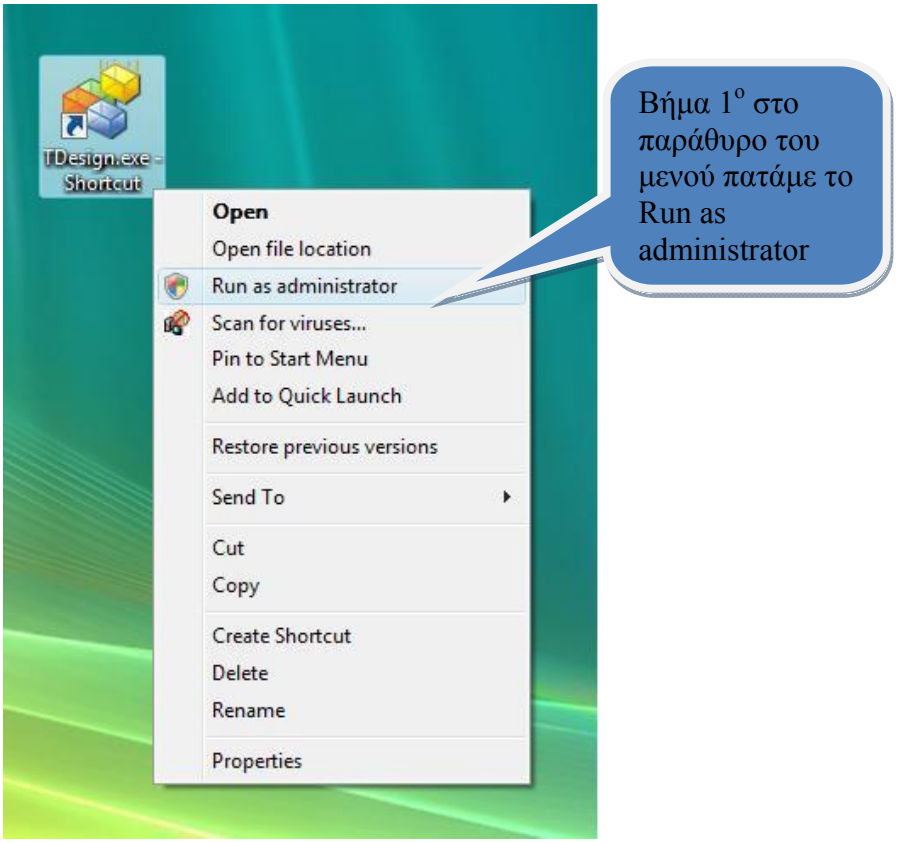
Είναι αξιοσημείωτο να σημειώσουμε ότι τα malware έχουν την δυνατότητα να ¨ζωγραφίσουν ¨ πάνω σε μια αλληλεπιδραστική επιφάνεια εργασίας , και να παρουσιάσουν έτσι μια μίμηση της ασφαλής επιφάνειας εργασίας , αλλά όταν τίθεται η ρύθμιση προτροπής για έγκριση το malware δεν θα έχει πετύχει τον προβιβασμό εκτός και αν ο χρήστης πέσει στην παγίδα και πατήσει το Continue στο παράθυρο της μίμησης αυτής . Ένα τώρα έχει τεθεί η ρύθμιση για προτροπή πιστοποιητικών , τα malware , μιμώντας την προτροπή των πιστοποιητικών μπορεί να καταφέρουν να συγκεντρώσουν τα πιστοποιητικά αυτά από τον χρήστη .
Σε αυτό το σημείο να αναφέρουμε ότι αυτά που προαναφέραμε δεν καθιστούν ικανά τα malware να κερδίσουν προνόμια καθώς το σύστημά μας διαθέτει και άλλους μηχανισμούς ασφάλειας οι

οποίοι είναι σε θέση να μετριάσουν τα malware από το να εισάγονται αυτόματα στην επιφάνεια εργασίας του χρήστη .

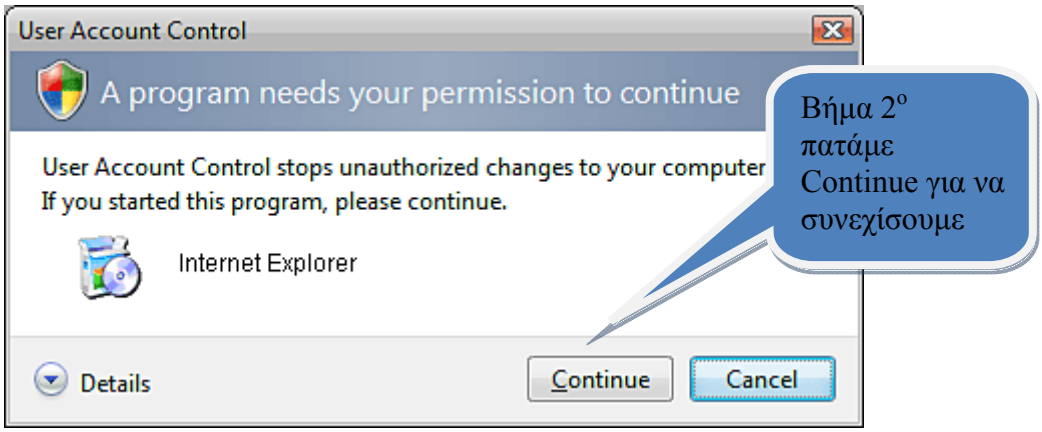
7.1.4.13 Εκτελώντας προγράμματα ως Διαχειριστής

Τα Windows Vista περιλαμβάνουν μια λειτουργία η οποία απαιτεί από μια εφαρμογή να ξεκινήσει να λειτουργεί χειροκίνητα. Για να εκτελέσουμε τώρα ένα πρόγραμμα με πλήρη διοικητικό σημείο πρόσβασης , ακολουθούμε τα παρακάτω αναλυτικά βήματα τα οποία μας παρέχουν την δυνατότητα αυτή :

I. Πατάμε **Δεξί κλικ** πάνω στο πρόγραμμα , το οποίο θέλουμε να τρέξουμε σαν διαχειριστές και επιλέγουμε την επιλογή **Εκτέλεση ως Διαχειριστής** .
II. Στο παράθυρο διαλόγου του UAC , επιλέγουμε **Συνέχεια.**



Εικόνα 60 : Παράθυρο Μενού .



Εικόνα 61 : Παράθυρο Διαλόγου UAC .

Μετά από την έγκριση της προτροπής από τον χρήστη , το πρόγραμμα θα αρχίσει να εκτελείται κανονικά και θα τρέχει με πλήρη διαχειριστικό σημείο πρόσβασης του χρήστη.

Για να μην επαναλαμβάνουμε την διαδικασία αυτή σε συγκεκριμένες εφαρμογές οι οποίες απαιτούν διαχειριστικά προνόμια μπορούμε να τις **¨σημειώσουμε¨** τις εφαρμογές αυτές και η διαδικασία να μην απαιτείται να εκτελεστεί .

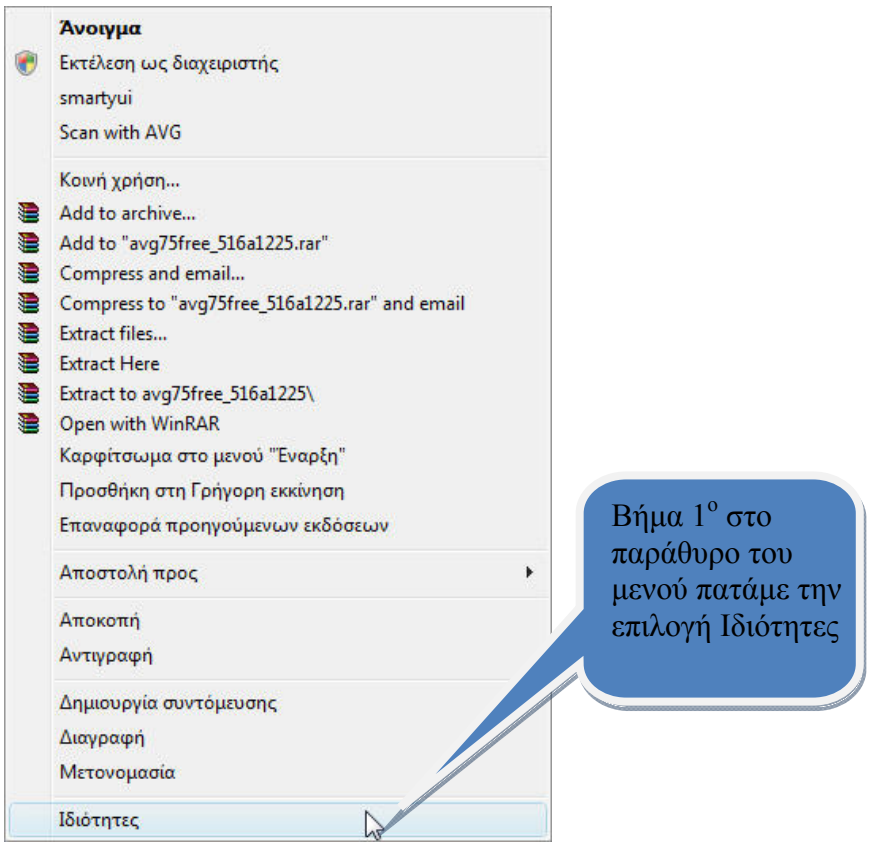
7.1.4.14 Πως ¨σημειώνουμε¨ εφαρμογές οι οποίες απαιτούν πλήρη διαχειριστή σημείο πρόσβασης

Υπάρχουν μερικές περιπτώσεις στις οποίες συγκεκριμένες εφαρμογές δεν λειτουργούν σωστά εκτός και αν τρέχουν μέσω ενός λογαριασμού οποίος διαθέτει πλήρη διαχειριστή σημείο πρόσβασης.
Αυτές οι περιπτώσεις μας απασχολούν συνήθως σε προ-Vista προγράμματα , τα οποία δεν είναι σχεδιασμένα να λειτουργούν κάτω από το UAC περιβάλλον .
Η Microsoft στην συνέχεια άρχισε να παρέχει έναν μηχανισμό, προκειμένου να εξασφαλίσει ότι αυτές οι εφαρμογές μπορούν να είναι ενεργές έτσι ώστε να έχουν πάντα την δυνατότητα να ¨σημειώνονται¨ όπως απαιτεί ένα πλήρες διαχειριστικό σημείο πρόσβασης .

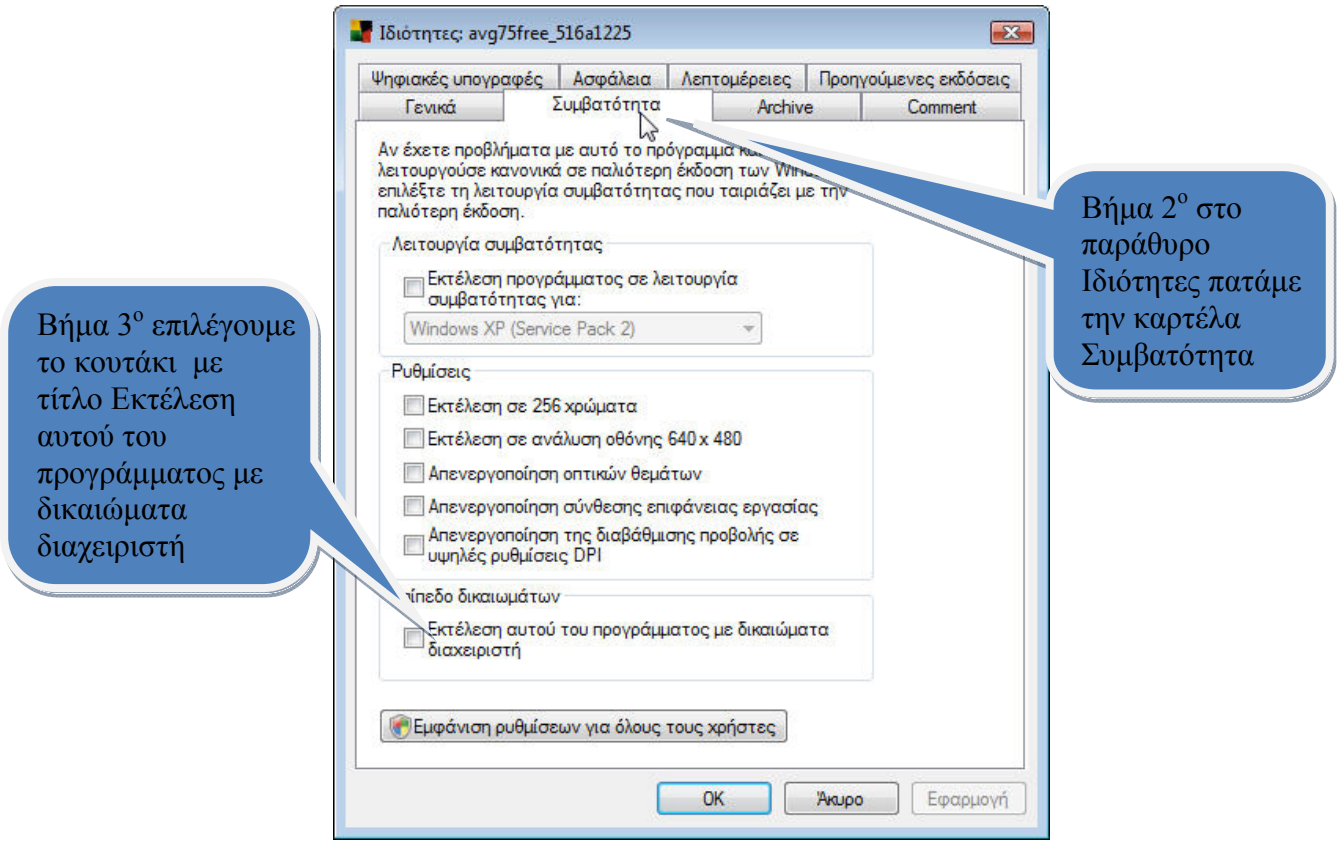
Η ακόλουθη διαδικασία περιγράφει πώς γίνεται το ¨μαρκάρισμα¨ μιας εφαρμογής , το οποίο μαρκάρισμα απαιτείται πάντα σε ένα πλήρες διαχειριστικό σημείο πρόσβασης :

1. Πατάμε **δεξί κλικ** στην εφαρμογή που επιθυμούμε να τροποποιήσουμε και επιλέγουμε τις **Επιλογές** .
2. Στην καρτέλα τώρα των επιλογών , διαλέγουμε την καρτέλα **Συμβατότητα** .
3. Στο κομμάτι του πλαισίου που φέρει τον τίτλο **Επίπεδο δικαιωμάτων** , τικάρουμε την επιλογή **Εκτέλεση αυτού του προγράμματος με δικαιώματα διαχειριστή** και στην συνέχεια πατάμε είτε **Εφαρμογή** είτε **OK.**
4. Την πρώτη φορά που θα γίνει το μαρκάρισμα μιας εφαρμογής , θα εμφανιστεί ένα κουτί διαλόγου .

5. Πατάμε **OK** για να συνεχίσουμε



Εικόνα 62 : Παράθυρο Μενού .



Εικόνα 63 : Παράθυρο Ιδιότητες .

7.1.5 Πως ρυθμίζουμε τον Γονικό Έλεγχο .

Ο τρόπος ρύθμισης του UAC διαφέρει από περίπτωση σε περίπτωση . Αυτό που εννοούμε είναι ότι ενώ η βασική ιδέα της λειτουργίας του καθώς και ο τρόπος που προστατεύει τους εκάστοτε χρήστες είναι ίδιος για όλες τις περιπτώσεις αυτό που αλλάζει είναι τα βήματα που εμείς σαν χρήστες ακολουθούμε προκειμένου να το ν ρυθμίσουμε . Στην συνέχεια θα ακολουθήσει λεπτομερή περιγραφή για κάθε μια από τις περιπτώσεις αυτές .

Στην παράγραφο αυτή θα ασχοληθούμε με το πώς ρυθμίζουμε τον UAC για ένα συγκεκριμένο περιβάλλον προγραμματισμού . Είναι σημαντικό να αναφέρουμε ότι το UAC επηρεάζει κάθε στοιχείο των Windows Vista που ο χρήστης χρησιμοποιεί .
Ο UAC είναι ένα ακέραιο συστατικό στης αρχιτεκτονική της ασφάλειας των Windows Vista .

Σε κάποια εταιρεία η Microsoft , συνέστησε να χρησιμοποιήσει μια **ομάδα πολιτικών (Group Policy)** καθώς και το **σύστημα Διαχείρισης του Server (SMS- Microsoft System Management Server)** , προκειμένου να διαχειρίζεται τον UAC .
Για υπολογιστές οι οποίοι δεν είναι μέλη ενός τομέα ή μέλη μιας ομάδας υπολογιστών , η Microsoft συνιστά την χρήση των αρχικών ρυθμίσεων του UAC μηχανισμού .

Με βάση τώρα τις προηγούμενες συστάσεις , το να επιλέξουμε ανάμεσα σε μια από δύο πιθανές μεθόδους προκειμένου να ρυθμίσουμε τα Windows Vista με τον UAC είναι :

- **Configure UAC for an enterprise workstation.**
- **Configure UAC for a home or unmanaged computer.**

- **Configure UAC for an enterprise workstation.**

Σε μια εταιρία , το να εξασφαλιστεί ότι οι χρήστες δεν έχουν την δυνατότητα να αλλάξουν τις ρυθμίσεις του συστήματος , να εγκαταστήσουν malware καθώς και να συμβιβάσουν οποιαδήποτε από τα δεδομένα των άλλων χρηστών , είναι κυρίαρχος στόχος .
Σαν αποτέλεσμα η Microsoft , συνιστά οι εταιρίες να ρυθμίσουν τις θέσεις εργασίας τους έτσι ώστε να λειτουργούν σαν τυποποιημένοι χρήστες .

Χρησιμοποιώντας τις ακόλουθες ρυθμίσεις θα βοηθηθούμε να ελαχιστοποιηθούν πιθανά προβλήματα :

- Ο UAC είναι ενεργός σε όλο το περιβάλλον και διατηρείται κυρίως μέσω του Group Policy .
- Η βάση του λογαριασμού του διαχειριστή διατηρείται ανενεργή και ένας κωδικός τίθεται προκειμένου να προφυλάξει οποιαδήποτε εκτός δικτύου επίθεση .
- Κάθε χρήστης της επιφάνειας εργασίας λειτουργεί με ένα δικό του λογαριασμό τυποποιημένου χρήστη .
- Η περιοχή του διαχειριστή διαθέτει δύο λογαριασμούς : έναν λογαριασμό τυποποιημένου χρήστη κα έναν λογαριασμό διαχειριστή στο Admin Approval Mode.
- Οι IT επεκτεινόμενες εφαρμογές χρησιμοποιούν το Microsoft System Management Server (SMS) , το Group Policy software installation (GPSI) , ή οποιαδήποτε άλλη παρόμοια εφαρμογή επεκτάσιμης τεχνολογίας . Εάν διαθέτουμε έναν UAC επεκτατικό μηχανισμό τοποθετημένο , η Microsoft συνιστά να θέτουμε εκτός λειτουργίας την ανίχνευση των εγκαταστάσεων των εφαρμογών .
- Το σημείο πρόσβασης προβιβασμού αντιμετωπίζεται από ένα help desk ή από ένα IT staff member είτε χρησιμοποιώντας την απομακρυσμένη βοήθεια είτε φυσικά εισάγοντας τα πιστοποιητικά στον υπολογιστή του χρήστη.

7.1.5.1 Configure UAC for a home or unmanaged computer.

Στο κομμάτι αυτό θα εξηγήσουμε πόσο πολύ βελτιώνεται εκτός από τις εταιρείες , την περίπτωση δηλαδή που προαναφέραμε , η ασφάλεια και στους προσωπικούς υπολογιστές , όταν είναι ενεργός ο UAC μηχανισμός .

Ενώ η ύπαρξη ενός λογαριασμού τυποποιημένου χρήστη υφίσταται από την περίοδο των Windows NT 4.0 οι περισσότεροι απλοί χρήστες είναι ανενημέρωτοι όσο αφορά το γεγονός της ύπαρξης διαφορετικών τύπων λογαριασμών .
Σαν αποτέλεσμα οι πλειονότητα των χρηστών σερφάρει στο web , επεξεργάζεται e-mail , αγοράζει on-line , καθώς και επεξεργάζεται έγγραφα σαν να είναι διαχειριστές . Επειδή ένας διαχειριστής διαθέτει πλήρη πρόσβαση σε πόρους του συστήματος , οποιοδήποτε κακόβουλο

λογισμικό το οποίο εγκαταστάτε στον υπολογιστή χωρίς την έγκριση μας , μπορεί να επηρεάσει αρχεία και φακέλους σε όλη την έκταση του υπολογιστή .

Μαζί με την παρουσίαση του UAC παρέχεται υποστήριξη μέσα στο λειτουργικό σύστημα και καθίσταται έτσι ευκολότερο για τους χρήστες να λειτουργούν σαν τυποποιημένοι χρήστες . Λειτουργώντας σαν τυποποιημένοι χρήστες είναι εγγενώς πιο ασφαλές και βοηθάει στο να περιοριστεί στο εύρος του συστήματος
η απώλεια δεδομένων λόγω της εγκατάστασης κακόβουλων λογισμικών .

Στο σημείο αυτό πρέπει να επιλέξουν οι χρήστες ένα από τους δύο ακόλουθους τρόπους ρυθμίσεων του περιβάλλοντος εργασίας του σπιτιού :

- Configure UAC with parental controls.
- Configure UAC without parental controls.

7.1.5.2 Configure UAC with parental controls

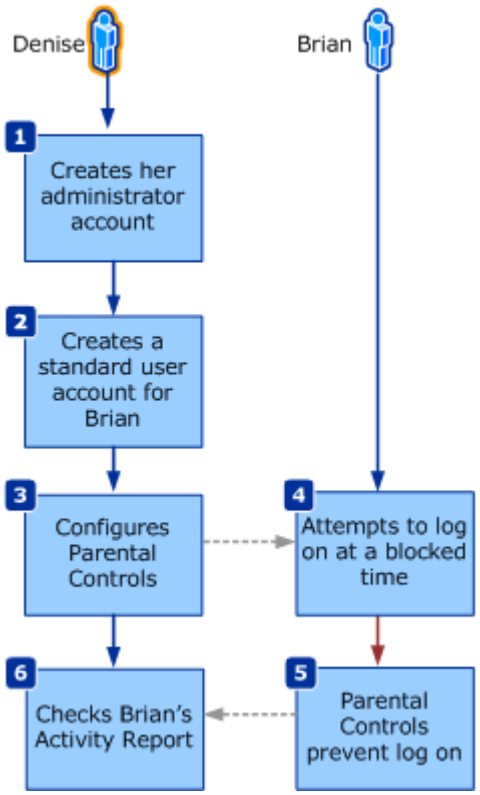
Το UAC καθιστά την ευέλικτη χρήση των γονικών ελέγχων , δηλώνοντας τις εργασίες και τους τύπους λογαριασμών των χρηστών .

Το παράθυρο ελέγχου του γονικού ελέγχου δεν εμφανίζεται στο Πίνακα ελέγχου του τομέα στον οποίο συμμετέχουν οι υπολογιστές .
Προτείνονται ατομικές ρυθμίσεις για την ενεργοποίηση του γονικού ελέγχου .

- Ο UAC να είναι ενεργός στον υπολογιστή .
- Όλοι ο γονικοί λογαριασμοί να δημιουργούνται ως διοικητικοί λογαριασμοί στο πλαίσιο του Admin Approval Mode .’
- Όλοι οι λογαριασμοί που απευθύνονται σε μικρά παιδιά να δημιουργούνται ως τυποποιημένοι λογαριασμοί .

Είναι ακόμη σημαντικό όλοι οι γονικοί λογαριασμοί να διαθέτουν ισχυρά passwords . Το πώς μπορούμε να δημιουργήσουμε ισχυρούς κωδικούς είναι ένα θέμα το οποίο μπορούμε να ενημερωθούμε μέσω του Web.

Το ακόλουθο διάγραμμα χρησιμοποιεί τα βέλη καθοδήγησης για να επεξηγήσει πώς ένας ¨γονιός¨ (διαχειριστής στο Admin Approval Mode) , μπορεί να ρυθμίσει γονικό έλεγχο για παιδιά .



Εικόνα 64 : Παράθυρο επεξήγησης ρύθμισης γονικού ελέγχου για παιδιά .

Στο προαναφερθέν σενάριο ο χρήστης Denise θέλει να ρυθμίσει γονικό έλεγχο στον υπολογιστή της, ο οποίος διαθέτει λειτουργικό σύστημα Windows Vista για να ελέγχει τι ώρα ο γιός της Brian μπορεί να έχει πρόσβαση στον υπολογιστή της .

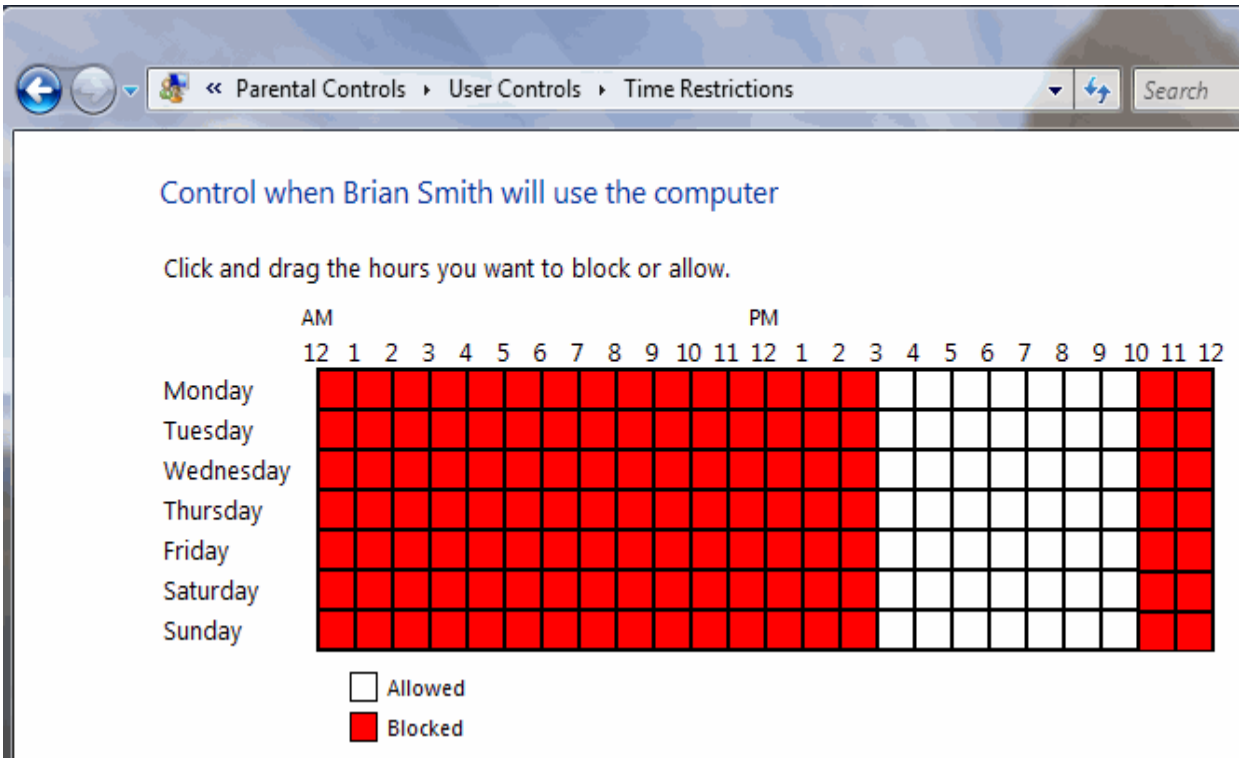
Πίνακας 5: Σενάριο γονικού ελέγχου χρήστη .

ΣΕΝΑΡΙΟ ΓΟΝΙΚΟΥ ΕΛΕΓΧΟΥ ΧΡΗΣΤΗ		
Όνομα	**Περιγραφή**	**Τύπος λογαριασμού χρήστη**
Brian	12 χρονών αγόρι , που παίζει παιχνίδια στον υπολογιστή και σερφάρει στο web.	Τυποποιημένος .
Denise	Μητέρα του Brian , η Denise θέλει να εξασφαλίσει ότι στον γιός της επιτρέπεται μόνο να εισάγεται στο σύστημα συγκεκριμένες ώρες .	Διαχειριστής χρήστης σε Admin Approval Mode .

1. Η Denise διαθέτει λειτουργικό Windows Vista και δημιουργεί έναν προσωπικό λογαριασμό στην αρχή κατά την διάρκεια της εγκατάστασης του λειτουργικού της .

Αυτός ο λογαριασμός δημιουργείται ως λογαριασμός τοπικού διαχειριστή με ενεργό τον UAC εξ ορισμού .

2. Η Denise τότε χρησιμοποιεί τον Πίνακα ελέγχου χρηστών για να δημιουργήσει ένα λογαριασμό τυποποιημένου χρήστη και την συνέχεια ανοίγει ο Πίνακας ελέγχου του γονικού ελέγχου .
3. Επειδή η Denise θέλει να εξασφαλίσει ότι ο γιος της δεν χρησιμοποιεί τον υπολογιστή αργά το βράδυ , χρησιμοποιεί τον γονικό έλεγχο για να σχεδιάσει χρονικά όρια , τα οποία επιτρέπουν στον Brian να εισάγεται στο σύστημα μόνο τις ώρες από 3 μμ μέχρι 10μμ .
   Η ακόλουθη εικόνα περιγράφει την ρύθμιση αυτή .



Εικόνα 65 : Παράθυρο ρύθμισης περιορισμού χρόνου .

4. Η Denise ενεργοποιεί την επιλογή της έκθεσης αναφορών , δηλαδή να λαμβάνει αναφορές σχετικά με τις δραστηριότητες του Brian , συμπεριλαμβανομένων τις σελίδες του web , τις οποίες ο Brian επισκέπτεται πιο συχνά ,τις ώρες εισαγωγής του και τα πιο πρόσφατα Web sites τα οποία είναι μπλοκαρισμένα από τον Γονικό έλεγχο .
5. Ο Brian επιχειρεί να εισέρθει στον υπολογιστή κάποια ώρα εκτός των επιτρεπτών πχ στις 10:30 μμ σαν αποτέλεσμα λαμβάνει ένα μήνυμα με την ακόλουθη μορφή ¨Ο λογαριασμός σας έχει περιορισμό χρόνου που σας απαγορεύει να κάνετε εισαγωγή αυτήν την ώρα . Παρακαλώ δοκιμάστε αργότερα¨.
6. Η Denise κάνει εισαγωγή στο σύστημα και παρακολουθεί την αναφορά δραστηριότητας του λογαριασμού του Brian.

Ο ακόλουθος πίνακας περιγράφει τις διαθέσιμες επιλογές του γονικού ελέγχου .

Πίνακας 6 : Windows Vista Γονικοί Έλεγχοι .

Windows Vista Γονικοί Έλεγχοι	
Γονικός Έλεγχος	**Περιγραφή**
Περιορισμοί στο Web	Γίνεται έλεγχος και επιτρέπεται η πρόσβαση ή όχι σε Web sites , downloads κα.
Χρονικοί περιορισμοί	Γίνεται έλεγχος όταν συγκεκριμένος χρήστης επιτρέπεται να χρησιμοποιήσει τον υπολογιστή .
Παιχνίδια	Γίνεται έλεγχος στα παιχνίδια με βάση τον τίτλο , το περιεχόμενο κα
Πρόσβαση και απαγόρευση εισόδου σε συγκεκριμένα προγράμματα	Επιτρέπει η μπλοκάρει οποιαδήποτε προγράμματα από το να λειτουργούν στον υπολογιστή μας
Αναφορά δραστηριοτήτων	Παρακολουθούμε τις αναφορές των δραστηριοτήτων

7.1.5.3 Configure UAC without parental controls

Η προτεινόμενη μέθοδος για ρύθμιση του UAC χωρίς γονικό έλεγχο για έναν υπολογιστή ο οποίος προορίζεται για σπίτι είναι παρόμοια με αυτήν της εταιρικής ρύθμισης , σενάριο που περιγράψαμε νωρίτερα.
Η λίστα που ακολουθεί , περιγράφει την προτεινόμενη ρύθμιση για υπολογιστή σπιτιού με λειτουργικό σύστημα Windows Vista .

- Δημιουργία ενός λογαριασμού διαχειριστή σε Admin Approval Mode.
- Δημιουργία ενός λογαριασμού τυποποιημένου χρήστη σαν πρωταρχικό λογαριασμό χρήστη .
- Δημιουργία όλων των ¨επόμενων ¨ λογαριασμών ως λογαριασμοί τυποποιημένων χρηστών .

Οι παρακάτω αναφορές περιγράφουν την λειτουργία ολοκλήρωσης των διαδικασιών που προαναφέραμε , την γενική εμπειρία των χρηστών και τέλος τις διάφορες μεθόδους ρύθμισης του UAC.

7.1.5.4 Δημιουργία ενός λογαριασμού διαχειριστή σε Admin Approval Mode.

Κατά την διάρκεια της διαδικασίας εγκατάστασης των Windows Vista , θα ζητηθεί από μας να παρέχουμε πληροφορίες σχετικές με την δημιουργία ενός χρήστη . Εξ ορισμού , ο λογαριασμός αυτός του χρήστη , δημιουργείται σαν ένας λογαριασμός διαχειριστή σε Admin Approval Mode.

7.1.5.5 Δημιουργία ενός λογαριασμού τυποποιημένου χρήστη σαν πρωταρχικό λογαριασμό χρήστη.

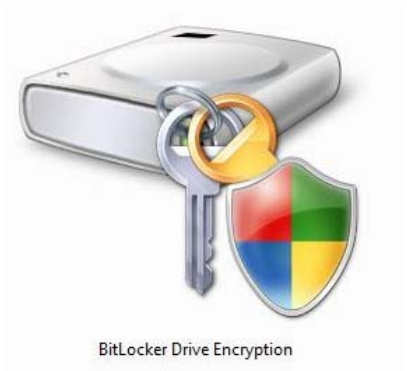
Η δημιουργία ενός τυποποιημένου χρήστη , πρέπει να ολοκληρωθεί αμέσως μετά που θα ολοκληρωθεί η διαδικασία της εγκατάστασης των Windows .
Για να δημιουργήσουμε έναν λογαριασμό τυποποιημένου χρήστη :

1. Κάνουμε εισαγωγή με έναν λογαριασμό διαχειριστή στο Admin Approval Mode .
2. Πατάμε **Έναρξη** , στην συνέχεια επιλέγουμε τον **Πίνακα Ελέγχου** και πατάμε **Προσθήκη ή κατάργηση λογαριασμών χρηστών.**\
3. Στο πλαίσιο διαλόγου του Γονικού Ελέγχου πατάμε **Συνέχεια**.
4. Στο πλαίσιο **Διαχείριση λογαριασμών** πατάμε **Δημιουργία ενός νέου λογαριασμού.**
5. Στο παράθυρο της Δημιουργία ενός νέου λογαριασμού που εμφανίζεται , πληκτρολογούμε το όνομα που θέλουμε να δώσουμε στον λογαριασμό αυτόν , και σιγουρευόμαστε ότι έχει επιλεγεί η επιλογή **Τυποποιημένος χρήστης**
6. Στην Διαχείριση λογαριασμών , πατάμε πάνω στον νέο αυτόν λογαριασμό που δημιουργήσαμε.
7. Στο παράθυρο **Αλλαγή ενός λογαριασμού** , πατάμε στην **Δημιουργία του κωδικού πρόσβασης** .
8. Εισάγουμε ένα πολύ δυνατό κωδικό και η διαδικασία έχει ολοκληρωθεί .

7.1.5.6 Δημιουργία όλων των ¨επόμενων ¨ λογαριασμών ως λογαριασμοί τυποποιημένων χρηστών

Κάθε επόμενος λογαριασμός χρήστη που δημιουργούμε μετά τους δύο πρώτους λογαριασμούς , θα πρέπει να είναι λογαριασμός τυποποιημένου χρήστη .
Η διαδικασία ορισμού του τύπου λογαριασμού των χρηστών θα γίνεται εξ ορισμού από τα Windows Vista χωρίς να χρειάζεται να κάνουμε εμείς καμία ενέργεια . Μόνο σε περίπτωση που επιθυμήσουμε να χρησιμοποιήσουμε κάποιον από αυτούς τους λογαριασμούς για προσωπική μας χρήση , θα πρέπει να ακολουθήσουμε τα βήματα που αναφέραμε στην προηγούμενη περίπτωση προκειμένου να επιφέρουμε οποιαδήποτε αλλαγή στις ρυθμίσεις του λογαριασμού αυτού .

7.2 Κρυπτογράφηση συστήματος - BITLOCKER DRIVE ENCRYPTION

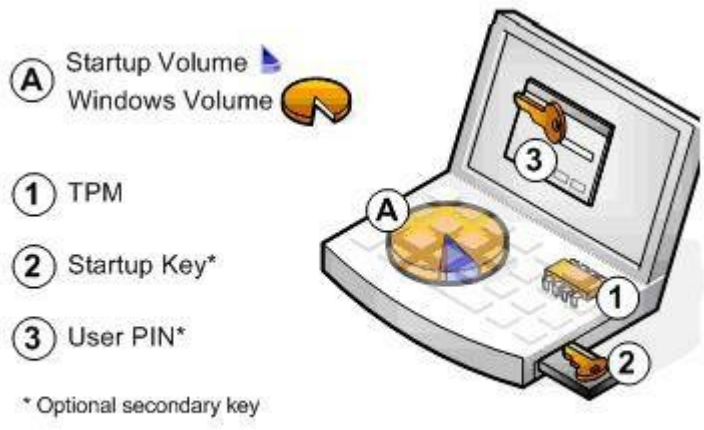


Με κύριο στόχο την καλύτερη κάλυψη των αναγκών τόσο των μεγάλων πολυεθνικών εταιριών όσο και εκείνων των οργανισμών που είχαν περίπλοκη υποδομή Η/Υ , η Microsoft κυκλοφόρησε μια νέα έκδοση των Windows , τα Windows Vista (Enterprise-Ultimate-Business). Οι εκδόσεις αυτές έχουν σχεδιαστεί έτσι ώστε να παρέχουν σημαντική μείωση του κόστους και των κινδύνων που ενέχει η χρήση υπολογιστών από πολλούς και διαφορετικούς χρήστες.
Παρέχουν εκτός από τις δυνατότητες που διαθέτουν τα Windows Vista Basic και Premium edition , και κάποιες έξτρα τεχνολογίες . Μια από αυτές είναι και το BitLocker Drive Encryption το οποίο με την χρήση τεχνολογίας κρυπτογράφησης που βασίζεται στον εξοπλισμό , παρέχει υψηλό επίπεδο προστασίας των δεδομένων. Επίσης ενσωματώνουν εργαλεία για την βελτίωση της συμβατότητας των εφαρμογών που μέχρι την παρούσα έκδοση(Ultimate) ήταν ένα σοβαρό πρόβλημα δυσλειτουργίας .
Η τεχνολογία κρυπτογράφησης Windows BitLocker , είναι ένα από τα νέα χαρακτηριστικά ασφαλείας των Windows Vista ,(καθώς επίσης και των Windows Server 2008) και το οποίο δεν υπήρχε στις προηγούμενες εκδόσεις των Windows , για αυτό και ίσως να είναι λίγο δυσνόητη η λειτουργία του . Παρακάτω γίνετε αναλυτική περιγραφή τόσο της λειτουργίας του όσο και των οφελών που αυτή παρέχει .
Η τεχνολογία Windows BitLocker έχει σαν βασική και πρωταρχική λειτουργία , την προστασία κρίσιμων δεδομένων ακόμη και σε φορητούς υπολογιστές που έχουν χαθεί ,κλαπεί , αποσυρθεί ή σε περιπτώσεις που έναν υπολογιστή τον μοιράζονται παραπάνω από ένας χρήστες πχ σε κάποια επιχείρηση , έτσι ώστε ούτε τα "ευαίσθητα " αυτά δεδομένα ούτε η πνευματική τους ιδιοκτησία να μην πέσουν σε λάθος χέρια . Με πλήρη κρυπτογράφηση δίσκου και έλεγχο ακεραιότητας το σύστημα BitLocker διασφαλίζει ότι τα δεδομένα του χρήστη δεν θα εκτεθούν σε κίνδυνο .
Το Windows BitLocker είναι ένα πλήρης (ή ολόκληρης όπως αλλιώς αναφέρεται), λογισμικό , κρυπτογράφησης δίσκων που βασίζεται στον εξοπλισμό .Ο όρος " πλήρης κρυπτογράφηση δίσκων " συχνά χρησιμοποιείται για να δηλώσει ότι όλα τα δεδομένα που οδηγούνται σε έναν δίσκο που εφαρμόζεται το BitLocker , κρυπτογραφούνται συμπεριλαμβανομένου και των αρχείων του λειτουργικού συστήματος .
Υπάρχουν βέβαια και άλλα προγράμματα που μπορούν να κρυπτογραφούν πλήρως τα δεδομένα σε έναν δευτερεύοντα δίσκο (πχ FreeOTFE, GBDE και το True Crypt) , αλλά δεν είναι ικανά να κρυπτογραφούν απευθείας το κομμάτι του συστήματος (system partition) ή το κομμάτι του boot (boot partition).
Αναφορικά θα πούμε ότι στην τεχνολογία των Microsoft Windows ,**System Partition** , σημαίνει κάποιο κομμάτι (partition) του δίσκου το οποίο περιλαμβάνει τα αρχεία τα οποία αναφέρονται **NTLDR,** και τα οποία ήταν απαραίτητα στις προηγούμενες εκδόσεις των Windows από Windows XP και παλαιότερα (Windows 98 , Windows 95 κτλ), προκείμενου να «μπουτάρει» το λειτουργικό μας σύστημα , δηλαδή να περάσει τις διαδικασίες ελέγχου που γίνονται στην αρχή

και να εισαχτεί στο περιβάλλον Windows. Στα Windows Vista χρησιμοποιείται ένα νέο αρχείο που ονομάζεται **bootmgr** το οποίο είναι τα αντίστοιχα NTDLR αρχεία και είναι διαμορφωμένο έτσι ώστε να εφαρμόζεται χρησιμοποιώντας το **BCDEdit.exe**.
Ενώ με την ονομασία **Boot Partition**, εννοείται ένα κομμάτι (partition) του δίσκου το οποίο περιλαμβάνει τα αρχεία του λειτουργικού συστήματος των Windows καθώς και τα αρχεία υποστήριξης γνωστά ως **support files**.
Το System Partition μπορεί να είναι σε διαφορετικό κομμάτι του δίσκου (partition) από το Boot Partition , παρόλα αυτά συχνά βρίσκονται στο ίδιο partition.
Ο Windows Installer δηλαδή το κομμάτι των Windows είναι υπεύθυνο για την εγκατάσταση του λειτουργικού συστήματος, τοποθετεί το αρχικό System Partition με βάσει τις ρυθμίσεις που του έχουν γίνει στο motherboard BIOS.
Το να «μπουτάρουμε» από ένα πλήρως κρυπτογραφημένο δίσκο σε ένα προσωπικό κομπιούτερ (personal computer) , απαιτείται η βοήθεια ειδικού υλικού (hardware) δεδομένου ότι δεν υπάρχει άλλος τρόπος για το BIOS, να αποκρυπτογραφηθεί και να μεταφερθεί ο έλεγχος προγράμματος (program control) σένα κρυπτογραφημένο **κύριο boot record (MasterBootRecord).**
Υπάρχουν , βέβαια προγράμματα που μπορούν να κρυπτογραφήσουν partition που χρησιμοποιούνται για εισαγωγή σε ένα λειτουργικό σύστημα , παρόλα αυτά τα προγράμματα αυτά θα πρέπει να αφήσουν πίσω το MBR , και έτσι μέρος του συστήματος θα παραμείνει μη κρυπτογραφημένο.

7.2.1 Τρόποι λειτουργιάς του Windows BitLocker.

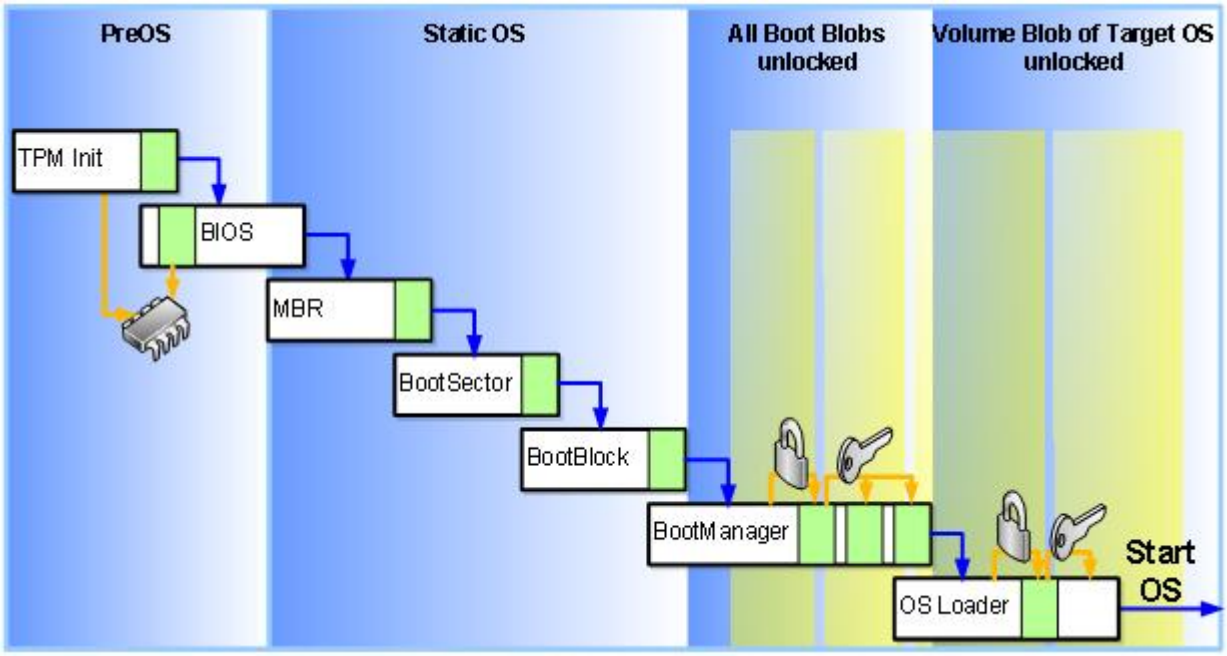
Το BitLocker παρέχει τρείς τρόπους λειτουργίας ,οι δύο πρώτοι απαιτούν για την εφαρμογή τους ένα κρυπτογραφικό υλικό και πιο συγκεκριμένα ένα τσιπ (cryptographic hardware chip), το οποίο ονομάζεται **Μονάδα Αξιοποίησης Πλατφόρμας - Trusted Platform Module** (έκδοσης 1.2 ή πιο πρόσφατη) καθώς και κάποιο συμβατό BIOS :



Εικόνα 66 : Παρουσίαση των τριών τρόπων λειτουργίας του Windows BitLocker .

i. Διαφανής Τρόπος Λειτουργίας (Transparent operation mode):

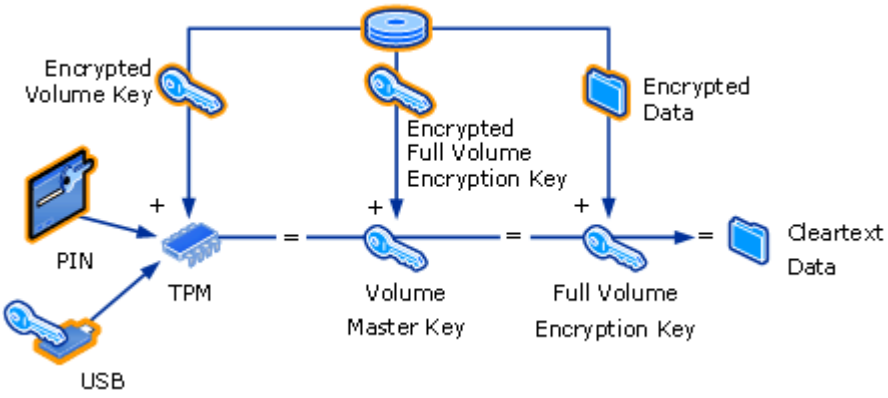
Αυτός ο τρόπος λειτουργίας εκμεταλλεύεται τις δυνατότητες του TPM προκειμένου να παρασχεθούν με ομαλό τρόπο σε έναν αρχικό χρήστη, τα εφόδια και οι εμπειρίες ασφαλείας των έμπειρων χρηστών πάνω στα Windows Vista .
Χρησιμοποιείται κάποιο κλειδί για την κρυπτογράφηση του δίσκου . Το κλειδί αυτό « σφραγίζεται » κρυπτογραφείται από το TPM chip , και απελευθερώνετε μόνο στον κώδικα του λειτουργικού συστήματος σε περίπτωση που τα προηγούμενα boot αρχεία εμφανιστούν χωρίς τροποποιήσεις. Τα προ-λειτουργικού συστήματος συστατικά (pre-OS components) του BitLocker επιτυγχάνουν αυτού του είδους την κρυπτογράφηση εφαρμόζοντας μια Static Root of Trust Measurement (μια μεθοδολογία που διακρίνει τους Trust Computing Group). Οι TCG είναι διάδοχοι της εμπιστευμένης συμμαχίας πλατφορμών υπολογισμού (TCPA) , και η οποία αρχικά ξεκίνησε από τις εταιρείες Intel,AMD, HP ,IBM ,Infineon,Microsoft και Syn Microsystems και οι οποίες εφάρμοσαν τεχνολογία Trust Computing.



Εικόνα 67 : Περιγραφή του Διαφανή τρόπου λειτουργίας του Bitlocker Drive Encryption .

ii. Τρόπος επικύρωσης χρηστών (User Authentication Mode):

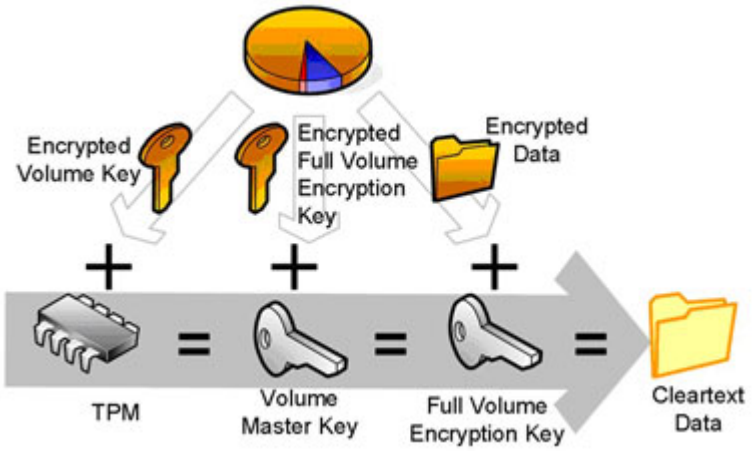
Αυτός ο τρόπος λειτουργίας απαιτεί ότι ο χρήστης θα παρέχει κάποια επικύρωση στο προ-boot περιβάλλον προκειμένου να επιτραπεί η έναρξη του λειτουργικού συστήματος (OS). Δύο ειδών επιβεβαιώσεις χρήστη υποστηρίζονται . Στην μια ένα προ – boot PIN εισάγεται από τον χρήστη και στην άλλη απαιτείτε η εισαγωγή μιας συσκευής USB η οποία περιέχει το απαραίτητο κλειδί ξεκινήματος (start up key).



Εικόνα 68 : Περιγραφή του τρόπου λειτουργίας του Bitlocker Drive Encryption με επικύρωση των χρηστών

iii. USB key:

Ο τρίτος τρόπος λειτουργίας δεν απαιτεί το TPM chip. Ο χρήστης πρέπει να εισάγει στο κομπιούτερ μια συσκευή USB η οποία περιέχει το κλειδί ξεκινήματος , προκειμένου να ξεκινήσει το προστατευμένο λειτουργικό σύστημα . Αυτός ο τρόπος λειτουργίας προαπαιτεί ότι το BIOS του προστατευμένου μηχανήματος θα υποστηρίζει και θα έχει τους κατάλληλους driver προκειμένου να είναι εφικτή η ανάγνωση του USB σε προ-λειτουργικό περιβάλλον .



Εικόνα 69 : Περιγραφή του τρόπου λειτουργίας του Bitlocker Drive Encryption με USB key.

7.2.2 Οδηγός Βήμα προς Βήμα του Windows BitLocker Drive Encryption

Αφού αναλύσαμε προηγουμένως για το τι ακριβώς είναι και τι κάνει το BitLocker Drive Encryption στο σημείο αυτό μέσω του οδηγού βήμα προς βήμα θα έρθουμε σε πρώτη επαφή με την λειτουργία του BitLocker .
Ο οδηγός αυτός περιέχει τις απαραίτητες οδηγίες χρήσης του Windows BitLocker Drive Encryption.Σαν σκοπό έχει να βοηθήσει τους διαχειριστές (administrator) κάθε συστήματος , να εξοικειωθούν με την νέα αυτήν τεχνολογία των Windows Vista .
Στα υποκεφάλαια που ακολουθούν παρέχονται οι βασικές πληροφορίες καθώς και οι ενέργειες που πρέπει οι administrator να προβούν προκειμένου να εγκαταστήσουν και να θέσουν για πρώτη φορά σε λειτουργία το BitLocker Drive Encryption .

7.2.2.1 Απαιτήσεις Υλικού Hardware για την Εγκατάσταση και χρήση του Windows BitLocker

Αρχικά γίνετε αναφορά στο υλικό που απαιτείται για την κρυπτογράφηση μονάδων δίσκου BitLocker .
Επειδή το πρόγραμμα BitLocker αποθηκεύει το δικό του κλειδί κρυπτογράφησης και αποκρυπτογράφησης σε μια συσκευή υλικού διαφορετική από τον δικό μας σκληρό δίσκο , θα πρέπει το σύστημα εκτός αυτού να διαθέτει ένα από τα εξής :

I. Ο υπολογιστής μας θα πρέπει να διαθέτει Μονάδα Αξιοποίησης Πλατφόρμας (TPM), η οποία είναι ένα ειδικό μικροτσίπ που υπάρχει σε ορισμένους νεώτερους υπολογιστές που υποστηρίζουν προχωρημένες δυνατότητες ασφάλειας . Εάν ο υπολογιστής που διαθέτουμε κατασκευάστηκε με TPM , έκδοσης 1.2 ή νεότερη , τότε το BitLocker θα αποθηκεύει το κλειδί του μέσα στην TPM.

II. Μια αφαιρούμενη συσκευή μνήμης USB ,όπως μια μονάδα **flash USB** .Εάν ο υπολογιστής μας δεν διαθέτει την TPM έκδοσης 1.2 ή νεότερη , τότε το BitLocker θα αποθηκεύει τα κλειδιά του στην μονάδα flash.

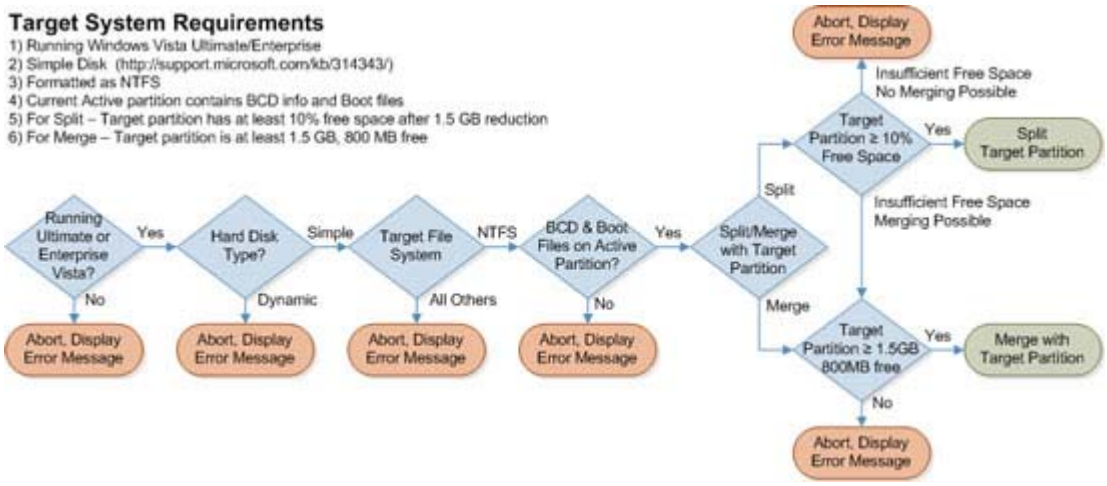
III. Για να ενεργοποιήσουμε την Κρυπτογράφηση μονάδων δίσκου BitLocker , ο σκληρός δίσκος του υπολογιστή μας θα πρέπει :

   i. Να έχει τουλάχιστον δύο διαμερίσματα (partition) 1,5 GB το καθένα .Το ένα διαμέρισμα περιλαμβάνει τη μονάδα δίσκου στην οποία είναι εγκατεστημένα τα Windows .Αυτή είναι και η μονάδα που θα κρυπτογραφήσει το BitLocker. Το άλλο διαμέρισμα είναι το ενεργό διαμέρισμα , το οποίο πρέπει να παραμείνει μη κρυπτογραφημένο έτσι ώστε να είναι δυνατή η εκκίνηση του υπολογιστή.

   ii. Να έχει διαμορφωθεί με το σύστημα αρχείων NTFS .

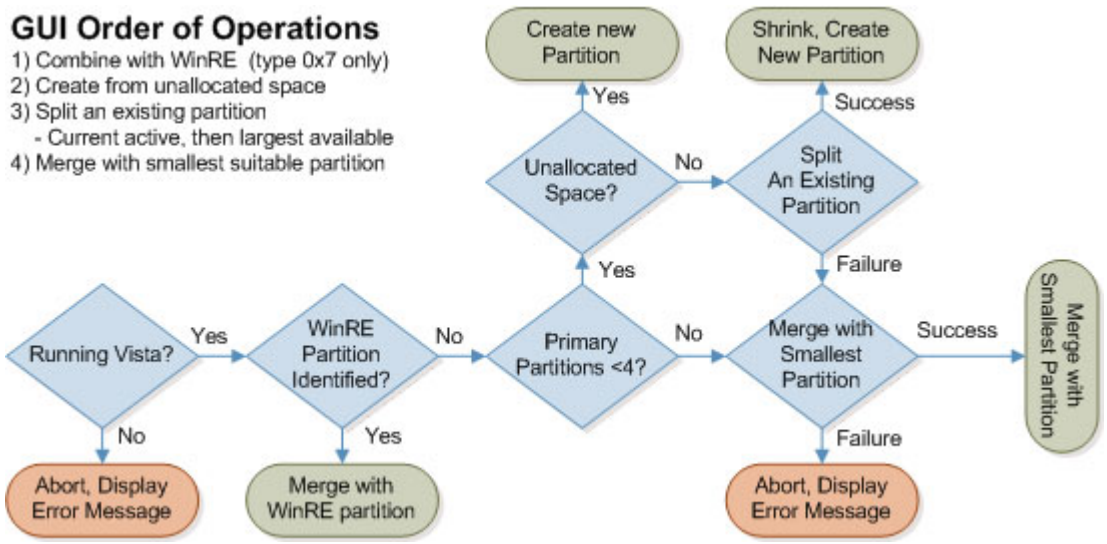
   iii. Να διαθέτει BIOS που είναι συμβατό με την TPM και να υποστηρίζει συσκευές USB κατά την εκκίνηση του υπολογιστή . Εάν δεν συμβαίνει

αυτό θα πρέπει να προβούμε στις απαραίτητες ενημερώσεις του BIOS πριν χρησιμοποιήσουμε το BitLocker.



Εικόνα 70 : Παρουσίαση των απαιτήσεων του συστήματος προσδιορισμού .

Το ακόλουθο γράφημα δείχνει την προτεινόμενη σειρά λειτουργιών την οποία ακολουθεί το εργαλείο προετοιμασίας μονάδων δίσκου BitLocker .



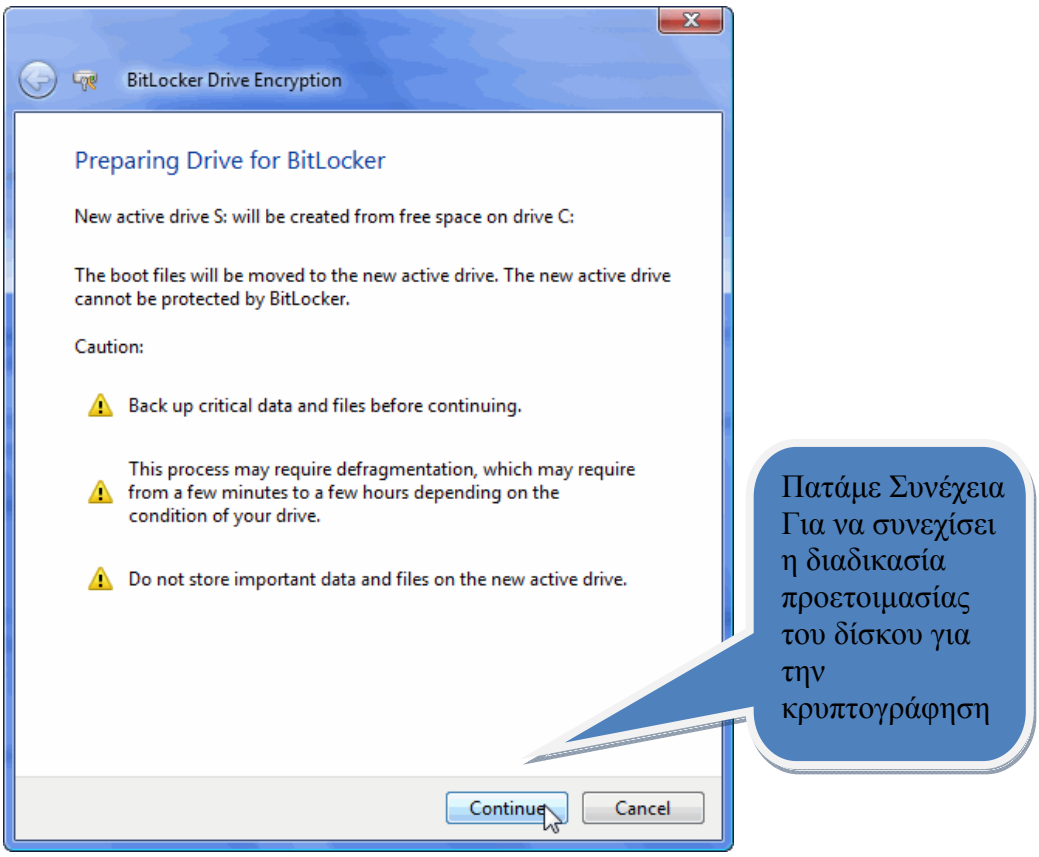
Εικόνα 71 : Παρουσίαση προτεινόμενης σειράς λειτουργιών του BitLocker .

7.2.2.2 Ενημέρωση του BIOS για την κρυπτογράφηση μονάδων δίσκου BitLocker

Αφού έγιναν γνωστές οι απαιτήσεις σε υλικό προκειμένου να γίνει εφαρμογή του BitLocker , τώρα θα αναφερθούμε στις ρυθμίσεις που πρέπει να γίνουν και στο λογισμικό που πρέπει να διαθέτουμε.
Όταν γίνει έναρξη για πρώτη φορά του BitLocker , ενδέχεται να εμφανιστεί ένα μήνυμα σφάλματος που θα μας ενημερώνει ότι πρέπει να γίνει ενημέρωση του βασικού συστήματος εισόδου εξόδου (BIOS) , προτού μπορέσουμε να χρησιμοποιήσουμε το BitLocker. Αυτό οφείλεται στο γεγονός ότι ο υπολογιστής διαθέτει από κατασκευής το υλικό ασφαλείας Μονάδα αξιόπιστης πλατφόρμας (TPM) και πρέπει να γίνει ενημέρωση του BIOS του υπολογιστή μας προκειμένου να λειτουργεί σωστά με την TPM . Εδώ θα πρέπει να σημειωθεί ότι αυτό το μήνυμα σφάλματος το λαμβάνουμε μόνο ένα πρωτίστως έχουμε κάνει αναβάθμιση σε αυτήν την έκδοση των Windows Vista από κάποιο παλαιότερο λειτουργικό σύστημα Windows.
Οι διαδικασίες για την αναβάθμιση του BIOS ποικίλουν ανάλογα με τον κατασκευαστή .Για να μάθουμε περισσότερα για κάμε μια από αυτές μπορούμε να ανατρέξουμε στο πληροφοριακό υλικό που συνοδεύει τον υπολογιστή μας ή να επισκεφτούμε την τοποθεσία Web του κατασκευαστή .

Σε περίπτωση τώρα που είναι ήδη ενεργοποιημένο το BitLocker και πρέπει να ενημερώσουμε το BIOS για κάποιον άλλο λόγο , όπως για να την επίλυση κάποιου προβλήματος συμβατότητας υλικού .Τα βήματα που πρέπει να ακολουθηθούν είναι τα εξής. Αρχικά πρέπει να απενεργοποιηθεί προσωρινά το BitLocker πριν γίνει ενημέρωση του BIOS, και στην συνέχεια αφού ολοκληρωθεί η ενημέρωση , γίνετε ενεργοποίηση ξανά του BitLocker. Αυτή η διαδικασία εμποδίζει το BitLocker να κλειδώσει την μονάδα δίσκου στην οποία είναι εγκατεστημένα τα Windows όταν , μετά την ενημέρωση , γίνει επανεκκίνηση του υπολογιστή .Αναλυτικά τώρα αυτό συμβαίνει γιατί εάν κατά την εκκίνηση του υπολογιστή το BitLocker εντοπίσει κάποια κατάσταση συστήματος που θα μπορούσε να αντιπροσωπεύει κάποιο κίνδυνο ασφαλείας (για παράδειγμα σφάλματα στον δίσκο , αλλαγή στο BIOS , ή αλλαγές σε οποιαδήποτε αρχεία εκκίνησης), θα κλειδώσει αμέσως την μονάδα δίσκου και για να την ξεκλειδώσουμε θα χρειαστούμε έναν ειδικό κωδικό αποκατάστασης BitLocker .
Αυτόν τον κωδικό αποκατάστασης θα πρέπει να έχουμε βεβαιωθεί ότι τον δημιουργήσαμε , και τον γνωρίζουμε, όταν ενεργοποιήσαμε για πρώτη φορά το BitLocker. Σε διαφορετική περίπτωση υπάρχει το ενδεχόμενο να χαθεί για πάντα η πρόσβαση στα αρχεία μας .
Μπορούμε να απενεργοποιήσουμε το BitLocker οποιαδήποτε στιγμή , είτε προσωρινά ,απενεργοποιώντας το ,είτε μόνιμα, αποκρυπτογραφώντας την μονάδα δίσκου.

7.2.2.3 Προετοιμασία του δίσκου για την κρυπτογράφηση μονάδων δίσκου BitLocker.



Εικόνα 72 :Παράθυρο προετοιμασίας δίσκου για τον BitLocker

Αφού κάναμε τις απαραίτητες ρυθμίσεις στο BIOS επόμενο βήμα είναι η προετοιμασία του σκληρού δίσκου για την ενεργοποίηση της κρυπτογράφησης BitLocker .
Όπως προαναφέραμε στο υποκεφάλαιο «Απαιτήσεις Υλικού Hardware για την Εγκατάσταση και χρήση του Windows BitLocker» , είναι υποχρεωτικό ο δίσκος του συστήματος μας να διαθέτει δύο τουλάχιστον διαμερίσματα (partitions) ,αυτό οφείλεται στον τρόπο λειτουργίας του BitLocker .
Το πρώτο partition το ονομαζόμενο system volume είναι αυτό το οποίο θα περιλαμβάνει της πληροφορίες του boot σε έναν μη κρυπτογραφημένο χώρο και το δεύτερο partition το οποίο ονομάζεται operating system volume , είναι αυτό το οποίο κρυπτογραφείται και το οποίο περιλαμβάνει τα δεδομένα του χρήστη και τα δεδομένα του λειτουργικού συστήματος .
Η κατάτμηση του δίσκου θα πρέπει να γίνει πριν την εγκατάσταση των Windows Vista .Αν πάλι έχει ήδη γίνει εγκατάσταση των Windows Vista , μπορούμε να χρησιμοποιήσουμε το εργαλείο BitLocker Drive Preparation Tool, για να διαμορφώσουμε και να προετοιμάσουμε τα partitions που χρειαζόμαστε για το BitLocker.

Κατάτμηση δίσκου για το BitLocker , χωρίς την ύπαρξη λειτουργικού συστήματος

Έστω ότι έχουμε στην κατοχή μας έναν απλό δίσκο , ο οποίος δεν έχει ακόμη χρησιμοποιηθεί οι ενέργειες στις οποίες πρέπει αν προβούμε είναι οι ακόλουθες :

i) Ξεκινάμε το σύστημά μας βάζοντας να μπουτάρει από το Σίντε των Windows Vista που έχουμε στην κατοχή μας .

ii) Στην αρχική οθόνη εγκατάστασης των Windows Vista (install window), επιλέγουμε την **γλώσσα εγκατάστασης** (installation language), την **τοπική ώρα** και τον **τόπο εφαρμογής** της ώρας (time and currency format) καθώς και την **γλώσσα πληκτρολογίου** (keyboard layout) και πατάμε **συνέχεια** (next) .

iii) Στην επόμενη οθόνη εγκατάστασης πατάμε την επιλογή **Επιδιόρθωση του συστήματος** (Repair your computer).

iv) Στις **Επιλογές του συστήματος επιδιόρθωσης** (System Recovery Options), βεβαιωνόμαστε ότι δεν υπάρχει επιλεγμένο κανένα λειτουργικό σύστημα.

v) Στις παράθυρο με τις επιλογές του Συστήματος επιδιόρθωσης , πατάμε το **Command prompt**.

vi) Μέσα τώρα στο command prompt πληκτρολογούμε την εντολή **disk part** και πατάμε **Enter** . Ανοίγουμε έτσι το εργαλείο **Κατάτμηση δίσκου** (Disk Part) για να δημιουργήσουμε ένα partition με μέγεθος τουλάχιστον 1,5 GB και το οποίο ορίζουμε ως κύριο (primary partition) .

vii) Πληκτρολογούμε **Select type 0** (για να το ορίσουμε ως κύριο).

viii) Πληκτρολογούμε **Clear** για να διαγραφούν όλα τα υπάρχοντα partitions (εάν υπάρχουν).

ix) Πληκτρολογούμε **Create partition primary size = 1500**, για αν ορίσουμε το μέγεθος του partition (μπορούμε να το ορίσουμε και παραπάνω από 1500 byte αυτή είναι η ελάχιστη τιμή που μπορούμε να του δώσουμε).

x) Στην συνέχεια πληκτρολογούμε **Assign letter = s** για να δώσουμε στο συγκεκριμένο partition το S ως αναγνωριστικό επιβεβαίωσης (σαν όνομα δηλαδή το οποίο θα το χαρακτηρίζει) .

xi) Ορίζουμε το partition αυτό ως ενεργό (active) πληκτρολογώντας την εντολή **Active**.

xii) Δημιουργούμε και ένα δεύτερο partition δίνοντας του τον υπόλοιπο χώρο που μας απομένει διαθέσιμος , πληκτρολογώντας **Create partition primary** .Μέσα στο οποίο θα εγκαταστήσουμε τα Windows αφού είναι το μεγαλύτερο σε χωρητικότητα .Καθώς επίσης του δίνουμε και αυτού ονομασία με την ίδια εντολή που δώσαμε και στο προηγούμενο , δηλαδή **Assign letter = c** .

xiii) Αφού ολοκληρώσουμε τις διαδικασίες αυτές για να βγούμε από την Κατάτμηση δίσκου πατάμε **Exit** .

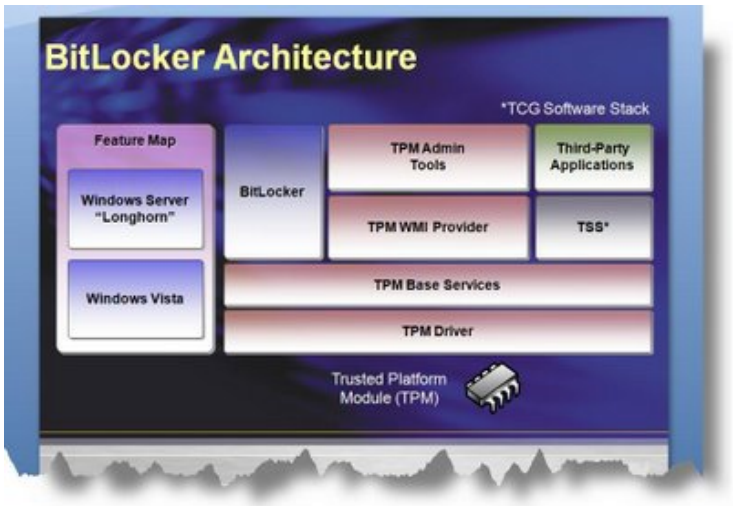
xiv) Στην συνέχεια φορμάρουμε και να δύο partitions ,με σύστημα αρχείων NTFS ,προκειμένου να μπορούν να χρησιμοποιηθούν σαν Windows volumes πληκτρολογώντας τις εντολές :

Format C: /y/q /fs: NTFS
Format S: /y/q /fs: NTFS

xv) Πατάμε **Exit** για να βγούμε και από το Command prompt.

xvi) Τέλος αφού κλείσουμε το παράθυρο του Recovery System Option (προσοχή ! δεν πρέπει να γίνει επανεκκίνηση του υπολογιστή μας), επιστρέφουμε στο αρχικό παράθυρο και πατάμε στην εντολή **Install Now** ,για να συνεχίσουμε με την εγκατάσταση των Windows Vista .

7.2.2.4 Αρχιτεκτονική του Windows BitLocker .



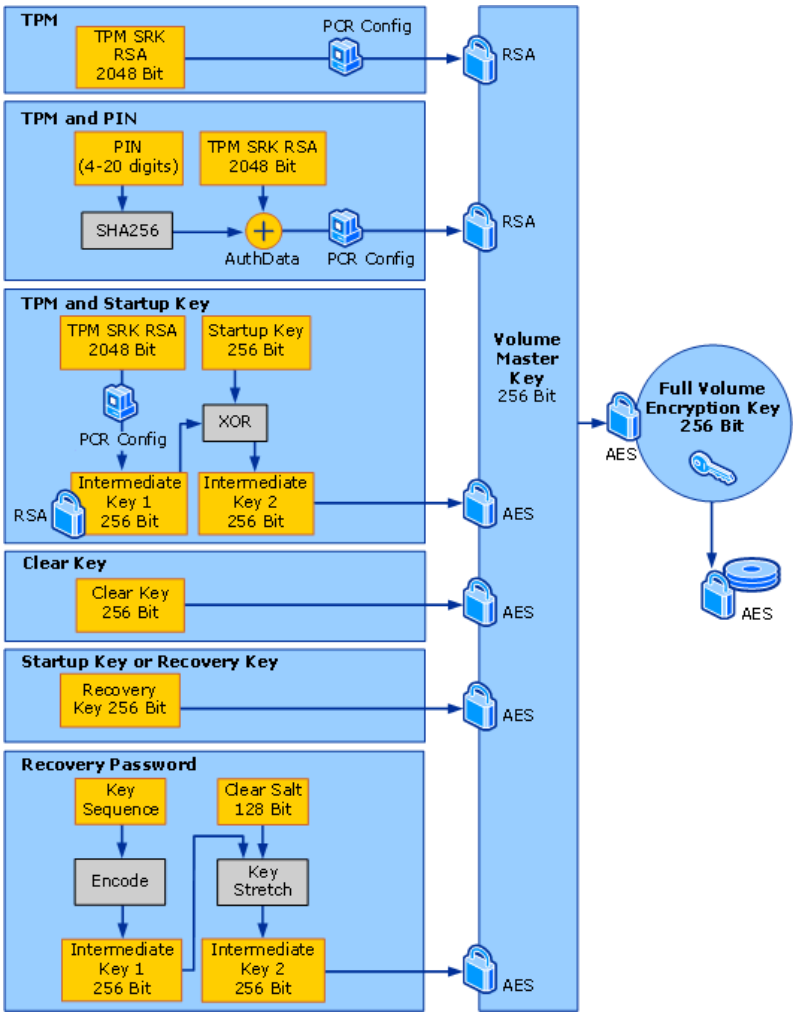
Εικόνα 73: Περιγραφή της αρχιτεκτονικής του BitLocker.

Ο μηχανισμός BitLocker , όπως προαναφέραμε , βοηθάει στο να προστατευτεί, το τμήμα λειτουργικού μας σύστημα στο σκληρό δίσκο , από μη εξουσιοδοτημένη πρόσβαση , κατά την διάρκεια που ο υπολογιστής μας είναι εκτός σύνδεσης . Για να επιτευχθεί αυτό , ο Windows BitLocker, χρησιμοποιεί πλήρους τμήματος κρυπτογράφηση (full –volume encryption) καθώς τις επεκτάσεις ασφάλειας που προσφέρονται από το TPM . Σημειώνουμε ακόμη ότι οι υπολογιστές οι οποίοι διαθέτουν TPM , ο BitLocker υποστηρίζει επίσης πολλών παραγόντων επικύρωση .

Ο BitLocker χρησιμοποιεί το TPM για να εκτελέσει τους ελέγχους ακεραιότητας συστημάτων στα κρίσιμα πρόωρα τμήματα του boot. Το TPM συλλέγει και αποθηκεύει τις μετρήσεις από τα πολλαπλά πρόωρα τμήματα boot και τα στοιχεία διαμόρφωσης των boot , για να δημιουργήσει ένα προσδιοριστικό συστήματος για εκείνο τον υπολογιστή , κάτι σαν ένα δακτυλικό αποτύπωμα . Εάν τα πρόωρα τμήματα των boot αλλάζουν ή πειραματίζονται , όπως για παράδειγμα η αλλαγή του BIOS , η αλλαγή του master boot record (MBR), ή ακόμη και η μετακίνηση του σκληρού δίσκου σε κάποιον άλλον υπολογιστή ,το TPM εμποδίζει τον BitLocker από το να κλειδώσει το κρυπτογραφημένο τμήμα και ο υπολογιστής εισάγει τον τρόπο αποκατάστασης .

Εάν το TPM ελέγξει την ακεραιότητα του συστήματος , ο BitLocker ξεκλειδώνει το προστατευμένο κομμάτι . Έπειτα το λειτουργικό σύστημα αρχίζει και η προστασία του συστήματος είναι πλέον ευθύνη του χρήστη και του λειτουργικού συστήματος .

Στο σχήμα που ακολουθεί επιδεικνύεται πως το BitLocker-προστατευμένο τμήμα κρυπτογραφείται με πλήρους τμήματος κρυπτογράφησης κλειδί , και το οποίο τμήμα στην συνέχεια κρυπτογραφείται με ένα κύριο κλειδί τμήματος (volume master key) . Η ασφάλιση του κύριου κλειδιού όγκου , είναι ένας έμμεσος τρόπος προστασίας των στοιχείων στο τμήμα . Η προσθήκη του κύριου κλειδιού όγκου επιτρέπει στο σύστημα να ξανακλειδώνει εύκολα , όταν τα κλειδιά της προς τα πάνω αλυσίδας εμπιστοσύνης χάνονται ή συμβιβάζονται .
Αυτή η δυνατότητα να επανεισαχθεί το σύστημα μας γλιτώνει από την δαπάνη της επανάληψης της κρυπτογράφησης και της αποκρυπτογράφησης ολόκληρου του όγκου .



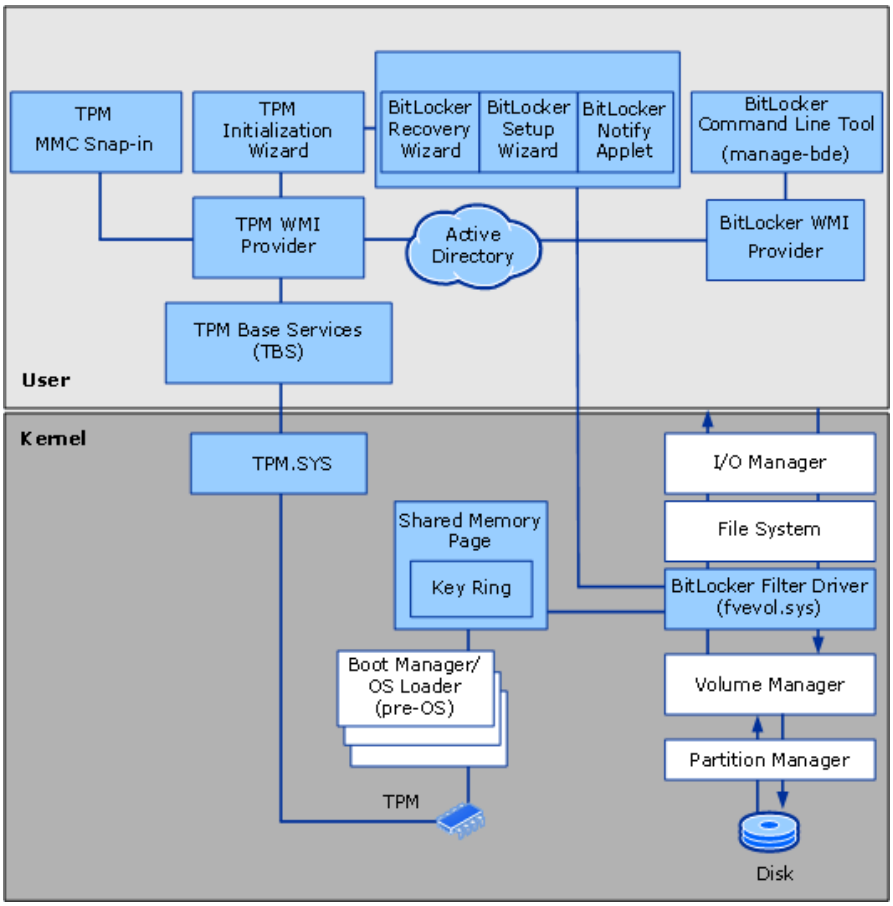
Εικόνα 74 : Περιγραφή της full-volume encryption .

Μόλις επικυρώσει ο BitLocker την πρόσβαση στον προστατευμένο όγκο του λειτουργικού συστήματος , ένας οδηγός φίλτρων στην σωρό των αρχείων των Windows Vista , κρυπτογραφεί και αποκρυπτογραφεί τους τομείς των δίσκων διαφανώς , όπως τα δεδομένα γράφονται και διαβάζονται από τον προστατευμένο όγκο . Όταν ο υπολογιστής διαχειμάζει , το αρχείο διαχείμασης σώζεται κρυπτογραφημένο στον προστατευμένο όγκο . Όταν ο υπολογιστής επαναλάβει την διαχείμαση , το κρυπτογραφημένο αρχείο διαχείμασης αποκρυπτογραφείται . Αφότου ο προστατευμένος όγκος κρυπτογραφηθεί από τον BitLocker κατά την διάρκεια της εγκατάστασης , ο αντίκτυπος ,της καθημερινής απόδοσης του συστήματος από την κρυπτογράφηση και αποκρυπτογράφηση, είναι ελάχιστος .

Εάν θέσουμε προσωρινά εκτός λειτουργίας τον BitLocker (παραδείγματος χάριν για να ενημερώσουμε το BIOS), ο όγκος του λειτουργικού συστήματος παραμένει κρυπτογραφημένος , αλλά το volume master key θα κρυπτογραφηθεί με ένα ¨καθαρό¨ κλειδί που θα αποθηκευτεί μη κρυπτογραφημένο στον σκληρό δίσκο . Η διαθεσιμότητα αυτού του μη κρυπτογραφημένου κλειδιού , θέτει εκτός λειτουργίας την προστασία των δεδομένων που παρεχόταν από τον BitLocker . Όταν ο BitLocker τεθεί και πάλι σε λειτουργία , το κλειδί αυτό αφαιρείται από τον δίσκο , το volume master key κλειδώνεται και κρυπτογραφείται και πάλι , και η προστασία BitLocker επαναλαμβάνεται .

7.2.2.4.1 Α. Διάγραμμα αρχιτεκτονικής.

Στο διάγραμμα που ακολουθεί παρουσιάζεται γενικά η αρχιτεκτονική του BitLocker , συμπεριλαμβανομένων των διάφορων μικρών εξαρτημάτων του . Επιδεικνύεται επίσης ο τρόπος των χρηστών και τον τρόπο των τμημάτων του πυρήνα του BitLocker , συμπεριλαμβανομένου του TPM , και του τρόπου ενσωμάτωσης με τα διαφορετικά στρώματα του λειτουργικού συστήματος .



Εικόνα 75: Περιγραφή του διαγράμματος αρχιτεκτονικής του BitLocker .

7.2.2.4.2 B. Τρόποι Επικύρωσης στην ακολουθία των boot .

Ο BitLocker υποστηρίζει τέσσερις διαφορετικούς τρόπους επικύρωσης , ανάλογα με τις ικανότητες του υλικού του υπολογιστή και το επιθυμητό επίπεδο ασφάλειας :

- BitLocker με TPM (χωρίς κανέναν πρόσθετο παράγοντα επικύρωσης).
- BitLocker με TPM και PIN.
- BitLocker με TPM και USB startup key
- BitLocker χωρίς TPM (απαιτείται USB startup key).

Κάθε φορά που ξεκινάνε τα Windows Vista , με ενεργοποιημένο τον BitLocker , ο κώδικας boot εκτελεί μια σειρά βημάτων βασισμένα στην ρύθμιση της προστασίας του volume . Αυτά τα βήματα μπορούν να περιλαμβάνουν , τους ελέγχους ακεραιότητας συστημάτων καθώς και άλλα βήματα επικύρωσης (PIN ή USB startup key) που πρέπει να ελέγχουν προτού κλειδωθεί το προστατευμένο volume .
Για λόγους αποκατάστασης , ο BitLocker χρησιμοποιεί ένα κλειδί αποκατάστασης (που αποθηκεύεται σε μια συσκευή USB) ή έναν κωδικό πρόσβασης αποκατάστασης (αριθμητικός κωδικός πρόσβασης). Το κλειδί αποκατάστασης ή ο κωδικός πρόσβασης αποκατάστασης ,

δημιουργείται κατά την διάρκεια της έναρξης του BitLocker . Η παρεμβολή του κλειδιού αποκατάστασης ή η δακτυλογράφηση του κωδικού πρόσβασης αποκατάστασης επιτρέπει σε έναν εξουσιοδοτημένο χρήστη να επανακτήσει την πρόσβαση στον κρυπτογραφημένο volume σε περίπτωση αποπειραθείσας παραβίασης διακοπής ή ασφάλειας του συστήματος.

Ο BitLocker πραγματοποιεί την αναζήτηση των κλειδιών με τα εξής βήματα :

1. **Το καθαρό κλειδί :** Η επαλήθευση ακεραιότητας συστημάτων έχει τεθεί εκτός λειτουργίας και το volume master key του BitLocker είναι ελεύθερα προσβάσιμο . Η επικύρωση δεν είναι απαραίτητη.

2. **Το κλειδί αποκατάστασης ή το startup(εάν παρουσιάζεται):** Εάν παρουσιάζεται είτε το κλειδί αποκατάστασης ή το κλειδί ξεκινήματος (start up) , ο BitLocker θα χρησιμοποιήσει άμεσα αυτό το κλειδί και δεν θα προσπαθήσει να ξεκλειδώσει το volume χρησιμοποιώντας άλλους τρόπους .

3. **Επικύρωση :**
    1. **TPM:** Το TPM επικυρώνει επιτυχώς τα πρόωρα τμήματα boot, για να ξεσφραγίσει το volume master key.

    2. **TPM και startup key:** Το TPM επικυρώνει επιτυχώς τα πρόωρα τμήματα boot, και ένα USB flash drive περιέχει το σωστό startup key το οποίο και εισάγεται.

    3. **TPM και PIN**: Το TPM επικυρώνει επιτυχώς τα πρόωρα τμήματα boot και ο χρήστης εισάγει το σωστό PIN.

4. **Αποκατάσταση :**

    1. **Κωδικός πρόσβασης αποκατάστασης :** Ο χρήστης πρέπει να εισάγει το σωστό κωδικό πρόσβασης αποκατάστασης .

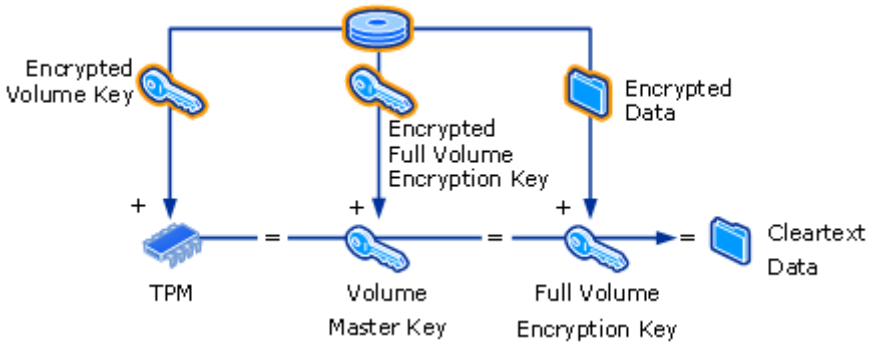
    2. **Κλειδί αποκατάστασης :** Εάν κανένα από τα ανώτερα βήματα δεν ξεκλειδώσουν επιτυχώς , ο χρήστης προτρέπεται να εισάγει ένα USB flash drive το οποίο διαθέτει τον κλειδί αποκατάστασης , και στην συνέχεια να επανεκκινήσει τον υπολογιστή .

Σενάριο – με χρήση του TPM μόνο .

Σε αυτό το σενάριο , ο BitLocker τίθεται σε λειτουργία σε έναν υπολογιστή που διαθέτει ένα TPM , αλλά κανέναν άλλος πρόσθετος παράγοντας επικύρωσης δεν είναι σε λειτουργία . Ο σκληρός δίσκος χωρίζεται σε δύο τόμους :

1. Το τόμο του συστήματος ,
2. Τον τόμο του λειτουργικού συστήματος των Windows Vista

Στο σχήμα που ακολουθεί ο BitLocker κρυπτογραφεί το λειτουργικό σύστημα με ένα full volume encryption key . Αυτό το ίδιο το κλειδί κρυπτογραφείται , με το volume master key , το οποίο στην συνέχεια κρυπτογραφείται από το TPM .



Εικόνα 76 : Παρουσίαση σεναρίου με χρήση TPM μόνο .

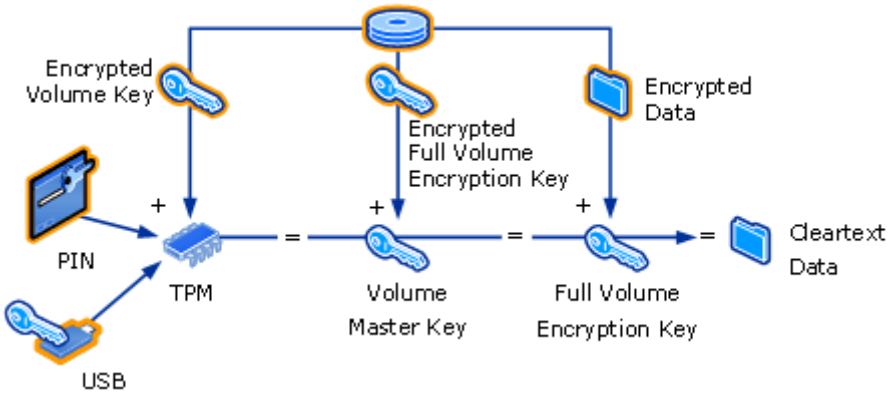
Αυτό το σενάριο μπορεί να επιτραπεί ή να τεθεί εκτός λειτουργίας από τον τοπικό διαχειριστή , χρησιμοποιώντας το στοιχείο ασφάλειας στον πίνακα ελέγχου των Windows Vista .Η απενεργοποίηση του BitLocker αποκρυπτογραφεί το volume και αφαιρεί όλα τα κλειδιά . Νέα κλειδιά δημιουργούνται μόλις ενεργοποιηθεί εκ νέου ο BitLocker .

Σενάριο – ενισχυμένης επικύρωσης .

Σε αυτό το σενάριο , προστίθενται επιπλέον παράγοντες επικύρωσης στο βασικό σενάριο που περιγράψαμε αρχικά . Όπως θα δούμε και στο σχήμα που ακολουθεί , ο BitLocker που χρησιμοποιείται σε έναν υπολογιστή που έχει ένα TPM προσφέρει δύο επιλογές πολυπαραγοντικής επικύρωσης :

- TPM και PIN (χρησιμοποιείται ο έλεγχος ακεραιότητας συστήματος συν κάτι που ο χρήστης ξέρει όπως ένα PIN).
- TPM και ένα startup key αποθηκευμένο σε κάποιον USB flash drive (χρησιμοποιείται ο έλεγχος ακεραιότητας συστήματος συν κάτι που ο χρήστης έχει).

Το πλεονέκτημα αυτού του σεναρίου είναι ότι δεν αποθηκεύεται όλο το βασικό υλικό στον τοπικό υπολογιστή .



Εικόνα 77: Παρουσίαση σεναρίου με ενισχυμένη επικύρωση .

Επικύρωση με χρήση ενός PIN.

Στο σενάριο αυτό, (όπως προαναφέραμε χρησιμοποιείται ο έλεγχος ακεραιότητας συστήματος συν κάτι που ο χρήστης ξέρει όπως ένα PIN), ο διαχειριστής δημιουργεί ένα αριθμητικό PIN κατά την διάρκεια έναρξης του BitLocker . Ο BitLocker κομματιάζει τον αριθμό PIN χρησιμοποιώντας ένα sha-256 και τα πρώτα 160bits του κομματιάσματος , χρησιμοποιούνται ως στοιχεία έγκρισης που στέλνονται στο TPM για να σφραγίσουν το κύριο κλειδί όγκου . Το κύριο αυτό κλειδί τώρα, προστατεύεται και από το TPM και από το PIN

Επικύρωση με χρήση ενός startup key.

Στο σενάριο αυτό , ο διαχειριστής δημιουργεί ένα κλειδί ξεκινήματος κατά την διάρκεια της έναρξης του BitLocker . Το κλειδί αποθηκεύεται σε μια BIOS- απαριθμημένη συσκευή αποθήκευσης όπως ένα pluggable USB flash drive , ο χρήστης από την μεριά του , θα πρέπει να εισάγει την συσκευή αυτή στον υπολογιστή , κάθε φορά που τίθεται σε λειτουργία ο υπολογιστής ή επανέρχεται από αδράνεια . Το USB flash drive που συγκρατεί το κλειδί ξεκινήματος , θα πρέπει να είναι συνδεμένο με τον υπολογιστή κατά την διαδικασία έναρξης , ενώ θα πρέπει να αφαιρείται μόλις τα Windows φορτώσουν .

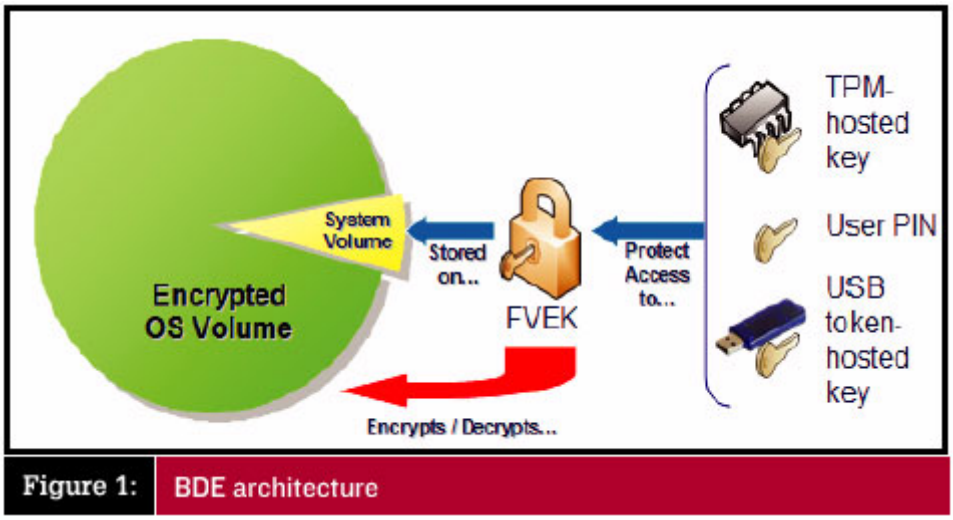
Σενάριο – με χρήση του startup key μόνο(χωρίς την παρουσία TPM) .

Σε αυτό το σενάριο, ο διαχειριστής θέτει σε λειτουργία τον BitLocker σε έναν υπολογιστή , οποίος δεν διαθέτει το TPM. Ο χρήστης του υπολογιστή αυτού , θα πρέπει να εισάγει ένα USB flash drive το οποίο περιέχει το startup key , και αυτό θα πρέπει να επαναλαμβάνεται κάθε φορά που επανεκκινείται το σύστημα ή επανέρχεται από μια κατάσταση αδράνειας .

Το startup key για το μη-TPM σύστημα , δημιουργείτε είτε κατά την διάρκεια της διαδικασίας της έναρξης είτε μέσω του οδηγού εγκατάστασης του BitLocker είτε μέσω του scripting .
Ο BitLocker παράγει το κλειδί του ξεκινήματος , ο χρήστης εισάγει το USB flash drive , και το σύστημα αποθηκεύει το startup key σε αυτήν την συσκευή .

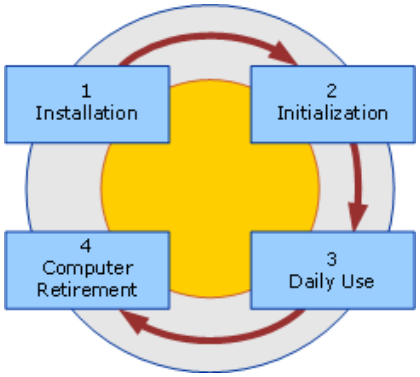
Χρησιμοποιώντας το στοιχείο του πίνακα ελέγχου του BitLocker , ο χρήστης μπορεί να δημιουργήσει ένα εφεδρικό αντίγραφο του κλειδιού ξεκινήματος . Το startup key αποθηκεύεται μη κρυπτογραφημένο , σε ένα αρχείο τύπου ¨.bek¨ ,σαν ακατέργαστα δυαδικά στοιχεία. Σε περίπτωση απώλειας του startup key , ο τόμος θα μπορεί να ανακτηθεί με την χρησιμοποίηση του κλειδιού αποκατάστασης και ένα νέο κλειδί ξεκινήματος θα πρέπει να παραχθεί (αυτή η διαδικασία θα ανακαλέσει το αρχικό κλειδί ξεκινήματος).

Όλοι οι άλλοι τόμοι που χρησιμοποιούσαν επίσης το χαμένο κλειδί ξεκινήματος , θα πρέπει να περάσουν από μια παρόμοια διαδικασία , ώστε να εξασφαλιστεί ότι το χαμένο κλειδί ξεκινήματος δεν θα χρησιμοποιηθεί από κανέναν αναρμόδιο χρήστη .



Εικόνα 78 :Παρουσίαση των τρόπων επικύρωσης του BitLocker .

7.2.2.4.3 Γ. Κύκλος ζωής του BitLocker .



Εικόνα 79 : Σχεδιάγραμμα κύκλου ζωής του BitLocker .

Υπάρχουν τέσσερα σημαντικά στάδια στον κύκλο ζωής του BitLocker , όπως φαίνεται και στο παραπάνω σχήμα . Τα στάδια αυτά περιλαμβάνουν , την εγκατάσταση , την έναρξη , την καθημερινή χρήση του υπολογιστή και τέλος τον αφοπλισμό ή ανακύκλωση του υπολογιστή .

1. **Εγκατάσταση :** Ο BitLocker είναι εγκατεστημένος ως τμήμα των Windows Vista ή ως προστιθέμενος ως επιλογή στον Windows Server 2008 .

2. **Έναρξη :** Ο BitLocker μονογράφεται και ενεργοποιείται .

3. **Καθημερινή χρήση :** Σενάριο ότι ο υπολογιστής χρησιμοποιείται σε καθημερινά. Ο BitLocker παρέχει ένα επίπεδο προστασίας βασισμένο στην επιλογή επικύρωσης που επιλέγεται κατά την διάρκεια της έναρξης .

4. **Αφοπλισμός και ανακύκλωση του υπολογιστή :** Ο BitLocker του υπολογιστή πρέπει να αφοπλιστεί ή να ανακυκλωθεί .

7.2.2.5 Έναρξη του BitLocker

Για να γίνει έναρξη του BitLocker,απαιτούνται να γίνουν τα παρακάτω βήματα :

I. Θα πρέπει να κάνουμε log on σαν administrator.

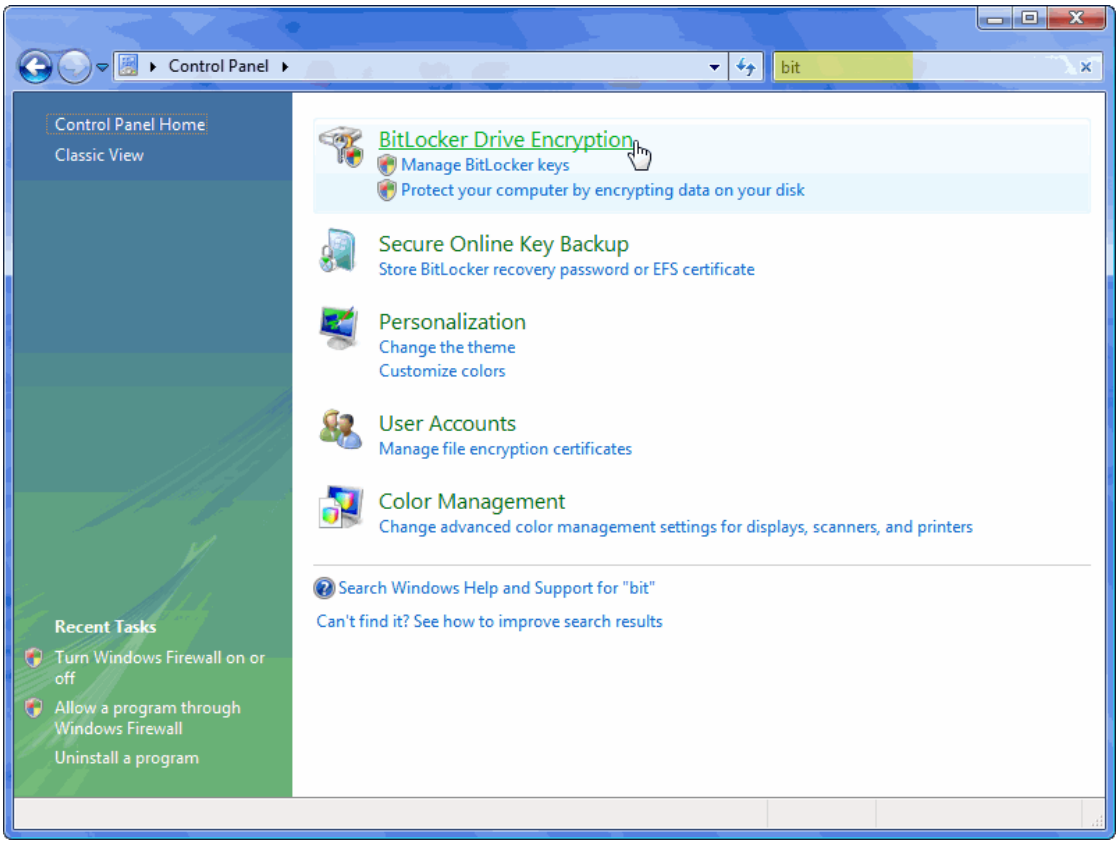
II. Αν μας ζητηθεί κωδικός πρόσβασης διαχειριστή ή επιβεβαίωση , πληκτρολογούμε τον κωδικό πρόσβασης ή την επιβεβαίωση .

Ανοίγουμε την Κρυπτογράφηση μονάδων δίσκου BitLocker κάνοντας κλικ στο κουμπί **Έναρξη,** έπειτα κάνουμε κλικ στον **Πίνακα Ελέγχου** , επιλέγουμε **Ασφάλεια ,** και στην συνέχεια , κάνουμε κλικ στην επιλογή **Κρυπτογράφηση μονάδων δίσκου BitLocker .**

III. Ίσως να εμφανιστεί ένα μήνυμα του User Account Control, για να επιβεβαιώσουμε την εντολή που ζητήσαμε να εκτελεστεί το προσπερνάμε πατώντας απλά στο κουμπί Συνέχεια .

IV. Στην σελίδα τώρα του BitLocker Drive Encryption , πατάμε στην εντολή Ενεργοποίηση του Windows BitLocker .

V. Εκτός από το ¨Προστασία του υπολογιστή με κρυπτογράφηση των δεδομένων στον δίσκο σας¨ , υπάρχει και η επιλογή ¨Διαχείριση κλειδιών BitLocker¨ , με την οποία ανοίγει η καρτέλα της Αποθήκευσης των κλειδιών κρυπτογράφησης (Save recovery password) .



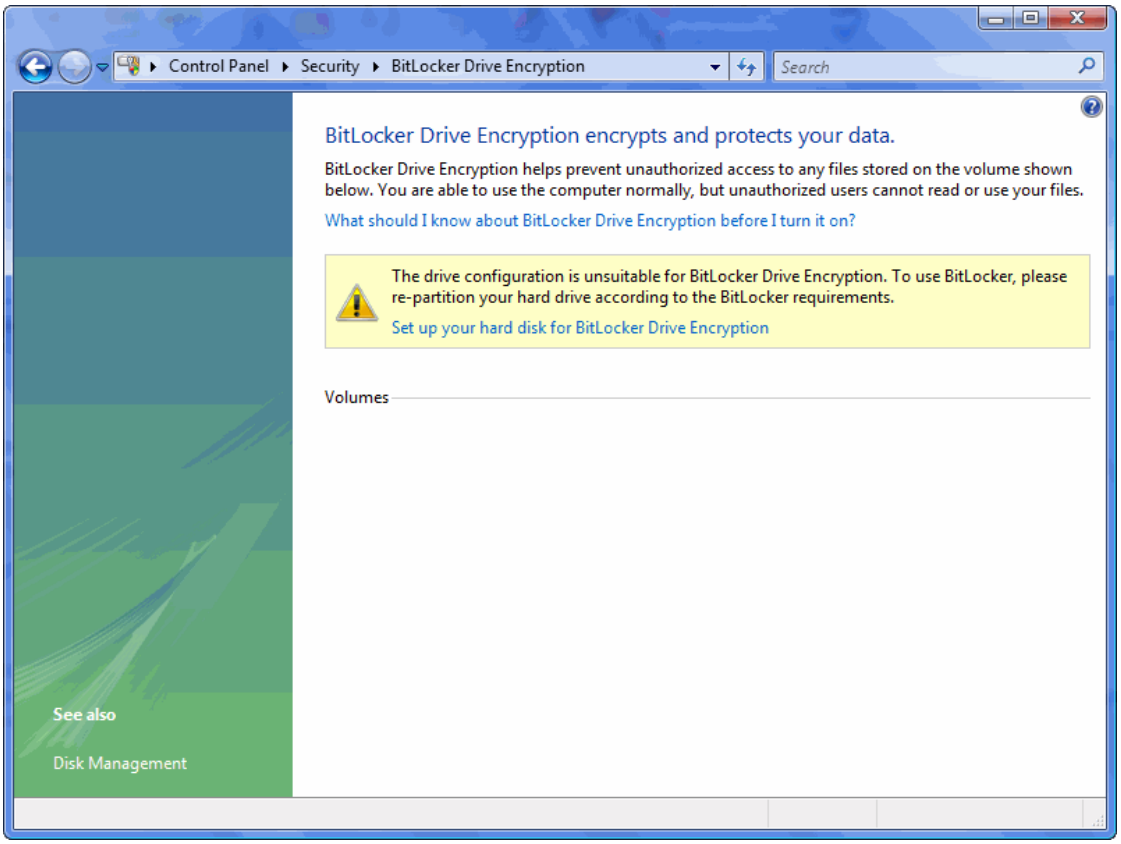
Εικόνα 80: Παράθυρο Έναρξης του BitLocker Drive Encryption .

Μέσα στην καρτέλα αυτή εμφανίζονται οι εξής επιλογές :

i. Αποθήκευση του κωδικού σε USB δίσκο. Επιλέγοντας αυτό το κλειδί της κρυπτογράφησης θα αποθηκευτεί σε ένα flash – USB δίσκο.

ii. Αποθήκευση του κωδικού σε έναν φάκελο . Με την επιλογή αυτή το κλειδί κρυπτογράφησης θα αποθηκευτεί σε έναν φάκελο τον οποίο έχουμε ορίσει εμείς εξ αρχής ρυθμίζοντας το BitLocker.

iii. Τέλος υπάρχει η επιλογή Εκτύπωση του Password .Στην περίπτωση αυτή ο κωδικός δεν αποθηκεύεται πουθενά μέσα στον υπολογιστή μας , απλά εκτυπώνεται και είναι ευθύνη του διαχειριστή να τον διασφαλίσει από επικείμενες απειλές .



Εικόνα 81 : Παράθυρο παρουσίασης των τόμων (volumes) του BitLocker .

Ανεξάρτητα από το ποια θα είναι η παραπάνω επιλογή μας , πρέπει να γίνει αντιληπτό ότι ο κωδικός κρυπτογράφησης καθώς και η προστασία του είναι πολύ σημαντικό ζήτημα . Ο κωδικός αυτός θα πρέπει να είναι γνωστός ανά πάσα στιγμή στον διαχειριστή του συστήματος γιατί θα του ζητηθεί σε οποιαδήποτε επόμενη ενέργεια κρυπτογράφησης και αν επιχειρήσει , ακόμη για μεγαλύτερη ασφάλεια θα ήταν προτιμότερο να αποθηκευτεί μακριά από το σύστημα στο οποίο έχει εφαρμοστεί .

VI. Η επόμενη καρτέλα είναι η Κρυπτογράφηση του επιλεγμένου δίσκου .Στην σελίδα αυτή επιβεβαιώνουμε ότι είναι επιλεγμένο το κουτάκι με τον τίτλο Έλεγχος συστήματος λειτουργίας του BitLocker . Εάν είναι επιλεγμένο πατάμε στο κουμπί Συνέχεια και κάνουμε επανεκκίνηση του συστήματος μας . Το σύστημα μας θα επανεκκινήσει και θα κάνει έλεγχο συμβατότητας προκειμένου να λειτουργεί σωστά ο BitLocker , εάν δεν εμφανιστεί κανένα μήνυμα λάθους η ενεργοποίηση του έχει γίνει σωστά , εάν τώρα εμφανιστεί κάποιο μήνυμα , εργαζόμαστε ανάλογα με το σφάλμα που μας έχει εμφανιστεί.

VII. Εφόσον πλέον έχει ενεργοποιηθεί η κρυπτογράφηση στο σύστημα μας , η μπάρα της διαδικασίας κρυπτογράφησης θα εμφανίζεται κάπου στην οθόνη μας . Μπορούμε να ελέγχουμε την ολοκλήρωση της διαδικασίας σέρνοντας το κέρσορα του ποντικιού μας πάνω στο εικονίδιο του BitLocker που βρίσκεται στο κάτω μέρος της οθόνης μας. Αφού

ολοκληρωθεί η διαδικασία αυτή έχει πλέον κρυπτογραφηθεί το σύστημα μας και ταυτόχρονα έχουμε δημιουργήσει το μοναδικό κλειδί αποκατάστασης του δίσκου αυτού .Από την επόμενη κιόλας φορά που θα κάνουμε log on στο σύστημα μας , τα δεδομένα μας θα κρυπτογραφούνται, παρόλα αυτά εμείς δε θα παρατηρούμε καμία απολύτως αλλαγή . Σε περίπτωση τώρα που κάποια στιγμή αλλάξει το TMP του συστήματος μας ή για κάποιον λόγο δεν μπορεί να έχει πρόσβαση στο σύστημα μας , εάν υπάρχουν αλλαγές στα βασικά αρχεία του συστήματος μας ή αν κάποιος προσπαθήσει να ξεκινήσει τον υπολογιστή μας , χρησιμοποιώντας κάποιον άλλο δίσκο με σκοπό να παρακάμψει το λειτουργικό μας σύστημα , σε μία από αυτές τις περιπτώσεις ο υπολογιστής αυτόματα θα μεταβεί σε κατάσταση αποκατάστασης και δεν θα έχουμε την δυνατότητα να κάνουμε την παραμικρή ενέργεια παρά μόνο εάν εισάγουμε τον κωδικό αποκατάστασης .

7.2.2.6 Προχωρημένες ρυθμίσεις χρήσης του BitLocker

Σε αυτό το κομμάτι θα αναφερθούμε σε προχωρημένες ρυθμίσεις που μπορούμε να κάνουμε στην κρυπτογράφηση BitLocker , προκειμένου να μπορούμε να την θέσουμε σε εφαρμογή ακόμη και εάν δεν διαθέτουμε το TPM ,ή να ενεργοποιήσουμε μια από τις προχωρημένες ρυθμίσεις έναρξης του BitLocker όπως πχ χρησιμοποιώντας το TPM με PIN, ή χρησιμοποιώντας το με κλειδί έναρξης (start up key).
Έστω ότι δεν διαθέτουμε TPM , το startup key με το οποίο γίνεται και η αυθεντικοποίηση μας θα πρέπει να είναι τοποθετημένο σε ένα Usb flash disk το οποίο θα πρέπει να το τοποθετήσουμε στον σύστημα μας πριν το θέσουμε σε λειτουργία .Σε μια τέτοια περίπτωση το BIOS του υπολογιστή μας θα πρέπει να είναι ρυθμισμένο ώστε να μπορεί να διαβάζει αυτό το USB δίσκο, σε προλειτουργικό περιβάλλον , δηλαδή πριν την εισαγωγή μας στα Windows Vista .
Για να ρυθμίσουμε την κρυπτογράφηση BitLocker έτσι ώστε να λειτουργεί με αυτόν τον τρόπο που αναφέραμε παραπάνω απαιτούνται τα παρακάτω βήματα :

Πριν Ξεκινήσουμε

i. Κάνουνε log on ως administrator.

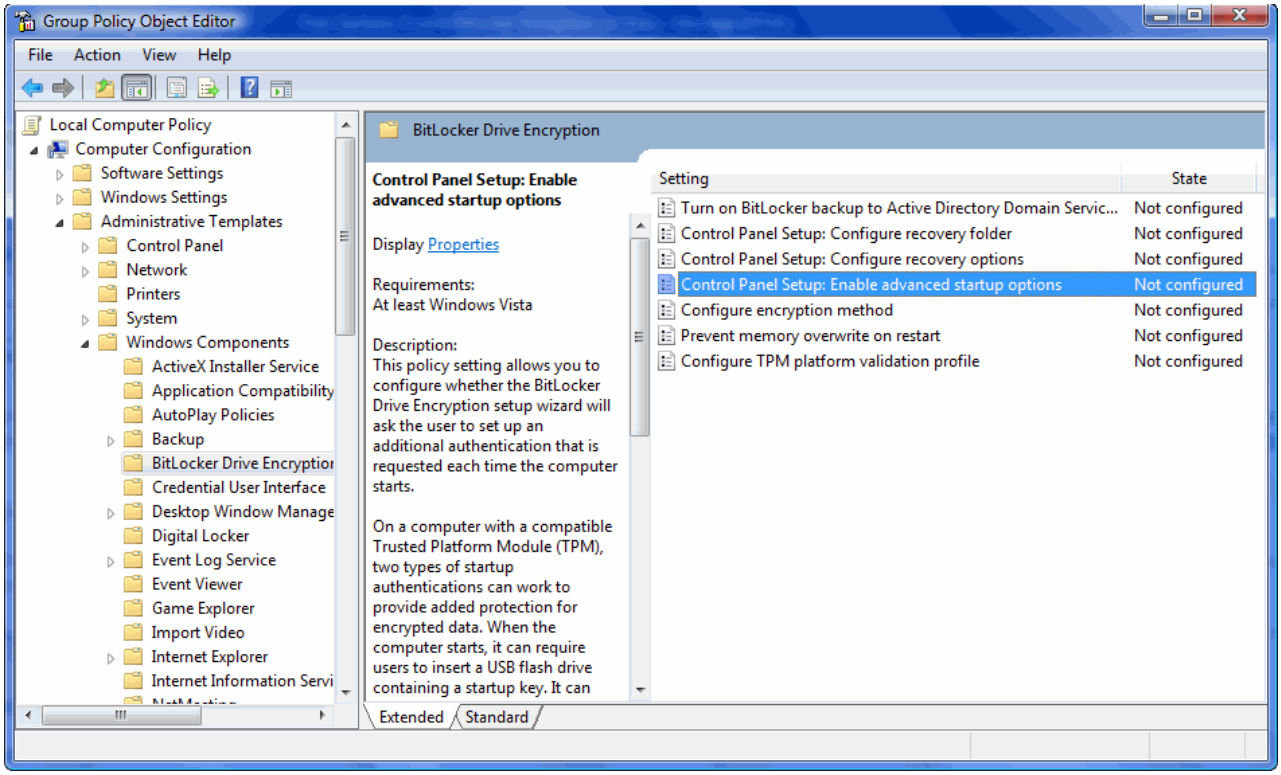
ii. Πρέπει να διαθέτουμε ένα Usb flash disk στο οποίο γίνει και η αποθήκευση του κωδικού . Καλό θα ήταν για λόγους ασφαλείας να διαθέτουμε παραπάνω από ένα USB , έτσι ώστε να μην αντιμετωπίσουμε κανένα πρόβλημα σε περίπτωση βλάβης του πρώτου.

Χρήση του BitLocker χωρίς να διαθέτουμε το TPM

i. Για να ανοίξουμε τώρα το BitLocker χωρίς να διαθέτουμε TPM , αρχικά πατάμε έναρξη και στο κουτί της **Έναρξης αναζήτησης** πατάμε την εντολή **gpedit. Msc** και μετά πατάμε **Enter**.

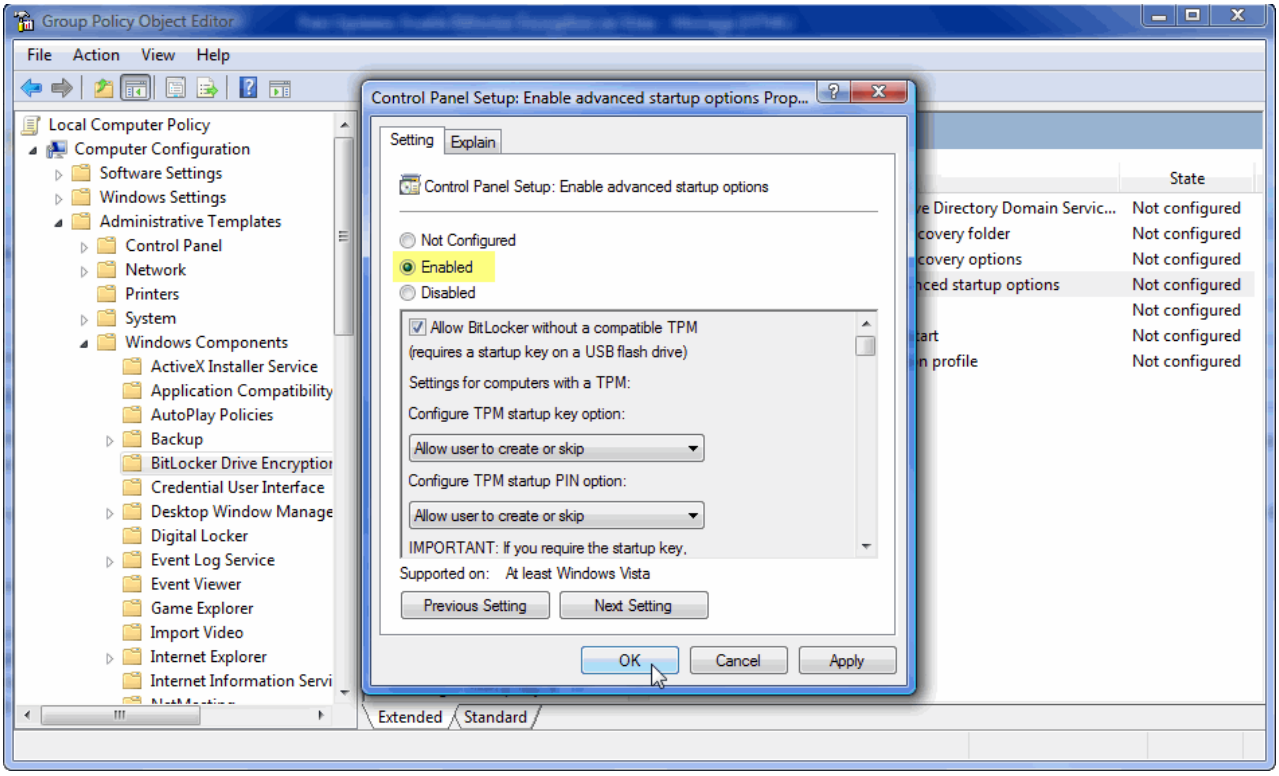
ii. Σε περίπτωση που μας εμφανιστεί το παράθυρο του User Account Control , επιβεβαιώνουμε την ενέργεια μας πατώντας στο κουμπί **Συνέχεια** .

iii. Στο παράθυρο του **Group Policy Object Editor** πατάμε κλικ στην εντολή **Local Computer Policy** , στην συνέχεια **Administrative Templates**, μετά **Windows Components** και τέλος διπλό κλικ στο **BitLocker Drive Encryption**.



Εικόνα 82 : Παράθυρο του Group Policy Object Editor .

iv. Στο επόμενο βήμα μας στον **πίνακα ελέγχου** πατάμε διπλό κλικ στο **Enable Advanced Startup Options** , θα εμφανιστεί το παράθυρο **Enable Advanced Startup Options** . Σε αυτό το παράθυρο θα τσεκάρουμε τα δύο κουτάκια με τίτλους **Enable option** και **Allow BitLocker without a compatible TPM** αντίστοιχα και στην συνέχεια πατάμε στο **OK** . Με αυτόν τον τρόπο έχουμε αλλάξει την πολιτική του συστήματος μας έτσι ώστε να μπορούμε να χρησιμοποιούμε κάποιο εξωτερικό κλειδί έναρξης αντί του TPM το οποίο δεν διαθέτουμε .



Εικόνα 83 : Παράθυρο ενεργοποίησης των προχωρημένων ρυθμίσεων.

v. Κλείνουμε το παράθυρο του Group **Policy Object Editor**.

vi. Μπορούμε ακόμη να «αναγκάσουμε» την πολιτική του συστήματος μας να εφαρμόσει άμεσα τις παραπάνω ρυθμίσεις ακολουθώντας μια δεύτερη τεχνική . Τα βήματα που ακολουθούμε είναι τα εξής : αρχικά πατάμε **Έναρξη** και στην συνέχεια γράφοντας την εντολή **gpupdate.exe / force** στο πλαίσιο της αναζήτηση και στην συνέχεια πατάμε **Enter**. Πατάμε **Έναρξη , Πίνακας Ελέγχου (Control Panel)** και μετά **BitLocker Driver Encryption** .Όπως και πριν περιμένουμε να ολοκληρωθεί η επεξεργασία αυτή και αφού μας εμφανιστεί και εδώ όπως και στην πρώτη περίπτωση το παράθυρο του **User Account Control** , πατάμε **Συνέχεια** για να επιβεβαιώσουμε τις ενέργειές μας .

vii. Έπειτα στο παράθυρο του **BitLocker Drive Encryption** πατάμε **Άνοιγμα του BitLocker (Turn on BitLocker)**

viii. **Στις ρυθμίσεις των προτιμήσεων έναρξης του BitLocker (Set BitLocker Startup Preferences)** , διαλέγουμε την επιλογή να απαιτείτε κλειδί έναρξης σε κάθε ξεκίνημα **(Startup USB key at ever startup)**.

ix. Σε περίπτωση τώρα , που δεν έχουμε ήδη εισάγει το usb κλειδί μας στο σύστημά μας το εισάγουμε και στην σελίδα **Αποθήκευση του Κλειδιού Έναρξης (You're your Startup key)** , πατάμε **Αποθήκευση (Save).**

x. Στην σελίδα Αποθήκευσης των κλειδιών κρυπτογράφησης (Save recovery password) παρατηρούμε ότι οι επιλογές που μας εμφανίζονται είναι ίδιες με αυτές που αναφέραμε και στη προηγούμενη περίπτωση (δηλαδή την αποθήκευσή του σε ένα Usb drive ,σε ένα φάκελο ή την εκτύπωση του) και τέλος πατάμε **Επόμενο (Next)** για να ολοκληρωθεί η αποθήκευση του.

xi. Τέλος αφού επανεκκινήσουμε το σύστημα έχουμε ολοκληρώσει πλήρως την διαδικασία και έχουμε θέσει σε εφαρμογή την κρυπτογράφηση BitLocker .

Έναρξη της κρυπτογράφησης BitLocker με χρήση TPM και PIN ή με TPM και με κλειδί έναρξης μέσω ενός USB flash drive

Σε αυτήν την περίπτωση θα μιλήσουμε για το πως μπορούμε να ρυθμίσουμε την κρυπτογράφηση μας έτσι ώστε να δουλεύει με έναν από τους παρακάτω συνδυασμούς , με χρήση TPM και PIN είτε με χρήση TPM και με κλειδί έναρξης μέσω ενός USB flash drive . Τα βήματα που ακολουθούμε είναι τα εξής:

i. Αρχικά πατάμε **Έναρξη** , στο πλαίσιο της **Έναρξης Αναζήτησης** πληκτρολογούμε την εντολή gpedit.msc και τέλος πατάμε Enter .

ii. Στην συνέχεια μας εμφανίζεται το παράθυρο User Account Control , στο οποίο και πατάμε Συνέχεια για να επιβεβαιώσουμε τις εντολές που έχουμε δώσει .

iii. Θα μας εμφανιστεί το παράθυρο με την ονομασία Πρόγραμμα επεξεργασίας αντικειμένου πολιτικής ομάδας , στο παράθυρο αυτό θα επιλέξουμε την καρτέλα Ρυθμίσεις του Χρήστη.

7.2.2.7 Encrypting File System

Το σύστημα κρυπτογράφησης αρχείων (EFS) , είναι ένας οδηγός αρχείων συστημάτων , ο οποίος χρησιμοποιεί κρυπτογράφηση επιπέδου file system , και είναι διαθέσιμος στα λειτουργικά συστήματα Microsoft Windows (2000 και τα νεώτερα) , εξαιρώντας τις εκδόσεις των λειτουργικών συστημάτων Windows XP Home Edition ,Windows Vista Basic, και τα Windows Vista Home Premium . Η τεχνολογία αυτή επιτρέπει διαφανώς στα αρχεία να είναι κρυπτογραφημένα με NTFS σύστημα αρχείων , για να προστατέψει με αυτόν τον τρόπο τα εμπιστευτικά μας στοιχεία από τους επιτιθέμενους μέσω της φυσικής πρόσβασης στον υπολογιστή .

Η επικύρωση του χρήστη καθώς και οι λίστες ελέγχου πρόσβασης μπορούν να προστατεύσουν τα αρχεία μας από την αναρμόδια πρόσβαση , καθώς τρέχει το λειτουργικό μας σύστημα, αλλά παρακάμπτονται εύκολα εάν ο επιτιθέμενος έχει καταφέρει να κερδίσει την φυσική πρόσβαση στο σύστημά μας .
Μια λύση για να αντιμετωπίσουμε αυτό , είναι να αποθηκεύουμε τα αρχεία κρυπτογραφημένα σε κάποιον δίσκο του συστήματος μας . Το EFS πραγματοποιεί την προαναφερθείσας λύση χρησιμοποιώντας την κρυπτογράφηση δημόσιου κλειδιού , στοχεύοντας να εξασφαλίσει ότι η διαδικασία της αποκρυπτογράφησης των αρχείων αυτών , να είναι θεωρητικά αδύνατη χωρίς το σωστό κλειδί . Εντούτοις , το EFS είναι στην πράξη ευαίσθητο σε επιθέσεις brute-force, που πραγματοποιούνται ενάντια στους κωδικούς πρόσβασης των λογαριασμών των χρηστών . Με άλλα λόγια η κρυπτογράφηση των αρχείων είναι μόνο τόσο ασφαλή όσο ο κωδικός πρόσβασης που ξεκλειδώνει το κρυπτογραφημένο κλειδί .

7.2.2.7.1 Πως λειτουργεί το Encrypting File System .

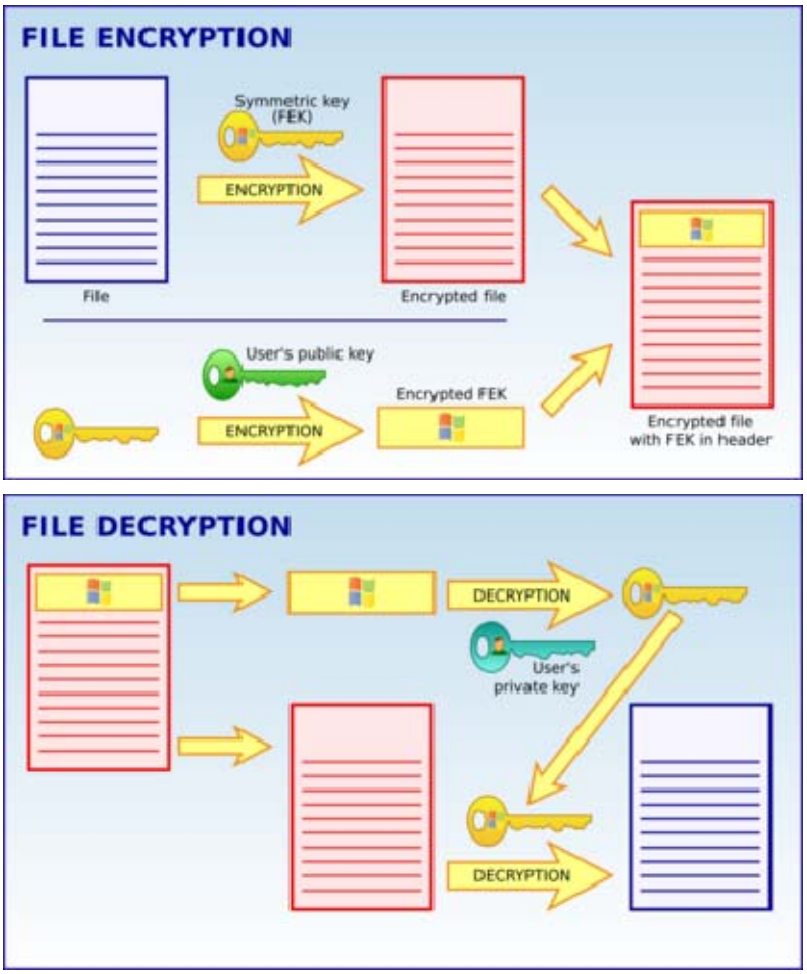
Το EFS λειτουργεί κρυπτογραφώντας ένα αρχείο με την χρήση ενός μαζικού συμμετρικού κλειδιού (symmetric key), το οποίο είναι γνωστό και ως Κλειδί Κρυπτογράφησης Αρχείων (File Encryption Key- FEK) . Χρησιμοποιεί ένα συμμετρικό αλγόριθμο κρυπτογράφησης για τον λόγο ότι παίρνει ένα σχετικά μικρότερο χρονικό διάστημα να κρυπτογραφηθούν και να αποκρυπτογραφηθούν μεγάλες ποσότητες δεδομένων , από ότι εάν χρησιμοποιούσαμε έναν cipher ασύρματου κλειδιού .
Ο συμμετρικός αλγόριθμος κρυπτογράφησης που χρησιμοποιείται ποικίλει ανάλογα με την έκδοση και την διαμόρφωση του εκάστοτε λειτουργικού συστήματος . Το FEK (το συμμετρικό κλειδί που χρησιμοποιείται για να κρυπτογραφηθεί το αρχείο) κρυπτογραφείται έπειτα με ένα δημόσιο κλειδί που συνδέεται με τον χρήστη που κρυπτογράφησε το αρχείο , και αυτό το FEK αποθηκεύεται στο $EFS εναλλασσόμενο
stream δεδομένων του κρυπτογραφημένου αρχείου.

Για να αποκρυπτογραφήσουμε το αρχείο, τα συστατικά του οδηγού EFS χρησιμοποιούν το ιδιωτικό κλειδί ,που ταιριάζει στο ψηφιακό πιστοποιητικό (το οποίο έχει χρησιμοποιηθεί για να κρυπτογραφηθεί το συγκεκριμένο αρχείο) για να αποκρυπτογραφήσουν το συμμετρικό κλειδί που έχει αποθηκευτεί στο $EFS εναλλασσόμενο stream δεδομένων . Τα συστατικά του οδηγού στην συνέχεια , χρησιμοποιούν το συμμετρικό κλειδί για να αποκρυπτογραφήσουν το αρχείο . Επειδή οι λειτουργίες της κρυπτογράφησης και της αποκρυπτογράφησης εκτελούνται σε ένα στρώμα κάτω από το NTFS , είναι διαφανές στον χρήστη και όλες τις εφαρμογές του.

Οι φάκελοι ,των οποίων τα περιεχόμενα πρόκειται να κρυπτογραφηθούν από το σύστημα αρχείων , είναι μαρκαρισμένοι με μια ιδιότητα κρυπτογράφησης . Τα συστατικά του οδηγού μεταχειρίζονται αυτήν την ιδιότητα κρυπτογράφησης με τρόπο ανάλογο της κληρονομικής άδεια στο NTFS . Εάν ένας φάκελος είναι μαρκαρισμένος ,για να κρυπτογραφηθεί , κατόπιν εξ ορισμού όλα τα αρχεία και οι υποφάκελοι κάτω από αυτόν τον φάκελο θα κρυπτογραφηθούν επίσης . Ακόμη όταν κάποια κρυπτογραφημένα αρχεία μετακινούνται μέσα σε έναν volume NTFS , τα αρχεία εξακολουθούν να παραμένουν κρυπτογραφημένα . Εντούτοις υπάρχουν διάφορες περιπτώσεις στις οποίες το αρχείο θα μπορούσε να αποκρυπτογραφηθεί , χωρίς να το απαιτεί ρητά ο χρήστης από τα Windows .

Οι φάκελοι και τα αρχεία αποκρυπτογραφούνται προτού να αντιγραφτούν σε κάποιο φορμαρισμένο volume το οποίο διαθέτει άλλο αρχείο συστήματος , όπως για παράδειγμα FAT32. Τέλος , όταν τα κρυπτογραφημένα αρχεία αντιγράφονται πάνω στο δίκτυο

χρησιμοποιώντας SMB/CIFS πρωτόκολλο , τα αρχεία αποκρυπτογραφούνται προτού αποσταλθούν μέσω του δικτύου .
Ο σημαντικότερος τρόπος για να αποτρέπουμε την αποκρυπτογράφηση αντιγράφων , είναι να χρησιμοποιούμε εφαρμογές backup οι οποίες έχουν γνώση του ¨RAW¨APIs.
Οι εφαρμογές backup οι οποίες έχουν γνώση του ¨RAW¨APIs ,αντιγράφουν απλά, τα κρυπτογραφημένα αρχεία stream και το $EFS εναλλασσόμενο stream δεδομένων , σαν να είναι κοινά αρχεία . Με άλλα λόγια τα αρχεία αυτά αντιγράφονται (σε backup) στην κρυπτογραφημένη τους μορφή , όπως είναι δηλαδή , και δεν αποκρυπτογραφούνται κατά την διάρκεια των backup.
Στο νέο λειτουργικό σύστημα των Windows Vista , το ιδιωτικό κλειδί του χρήστη , μπορεί να αποθηκευτεί σε μια έξυπνη κάρτα , ακόμη και το Data Recovery Agent (DRA) κλειδί μπορεί και αυτό να αποθηκευτεί σε μια έξυπνη κάρτα .



Εικόνα 84 : Περιγραφή της διαδικασίας κρυπτογράφησης και αποκρυπτογράφησης .

7.2.2.8 Κρυπτογράφηση μονάδων δίσκου BitLocker VS Σύστημα αρχείων κρυπτογράφησης EFS

Η πλήρης κρυπτογράφηση δίσκου έχει πολλά προνόμια έναντι του συστήματος κανονικής κρυπτογράφησης αρχείων ή φακέλων ή από τους κρυπτογραφημένους vaults, παρακάτω ακολουθούν μερικά από αυτά :

i. Όλα συμπεριλαμβανομένου του χώρου ανταλλαγής (swap space) και των πρόχειρων φακέλων

(temporary files) , κρυπτογραφούνται . Το να κρυπτογραφούνται αυτού του είδους τα αρχεία είναι πολύ σημαντικό διότι μέσω αυτών μπορούν να αποκαλυφθούν σημαντικά και εμπιστευτικά προσωπικά στοιχεία.

ii. Με την πλήρη κρυπτογράφηση η απόφαση των ποιών αρχείων κρυπτογραφούνται δεν αφήνεται πλέον στους χρήστες .

iii. Παρέχει υποστήριξη για την επικύρωση των pre-boot.

iv. Τέλος παρέχει μεγαλύτερη ασφάλεια με την άμεση διαγραφή δεδομένων, όπως του κλειδιού κρυπτογράφησης συστήματος (cryptography keys) καθιστώντας έτσι τα κρυπτογραφημένα με αυτό αρχεία άχρηστα στους μη γνώστες αυτού . Εντούτοις αν μας απασχολεί η ασφάλεια μας από μελλοντικές επιθέσεις που ίσως δεχτούν τα «κρίσιμα αρχεία » μας , ένα καλό μέτρο είναι η φυσική καταστροφή τους, καθώς επίσης και το « σκούπισμα αρχείων » (file wiping) .

7.3 Windows service hardening

Στην προσπάθεια της η Microsoft να γίνει πιο ασφαλής από ποτέ έχει συμπεριλάβει στο νέο λειτουργικό της μια σειρά από νέα χαρακτηριστικά ασφαλείας . Τα χαρακτηριστικά αυτά είναι σχεδιασμένα με τέτοιο τρόπο ώστε να αντιμετωπίζουν τόσο τις καθημερινές και κοινές απειλές που μπορεί να αντιμετωπίσει ο οποιοδήποτε χρήστης όσο και τις νέες και εξεζητημένες απειλές .

Ένα τέτοιο νέο χαρακτηριστικό των Windows Vista είναι γνωστό ως Windows Service Hardening ή αλλιώς Υπηρεσία Hardening των Windows.
Ρόλος του χαρακτηριστικού αυτού είναι να αποτρέψει τις Υπηρεσίες Windows (Windows Services) , από το να κάνουν οποιαδήποτε είδους αλλαγές στα αρχεία του συστήματος (Files System) , στην registry ή στα δίκτυα του συστήματος μας οι οποίες αλλαγές δεν θα έπρεπε να συμβούν . Με αυτόν τον τρόπο μειώνονται οι συνολικές **επιθέσεις επιφάνειας** στο σύστημα μας καθώς παρεμποδίζεται η είσοδος των malware των οποίων απώτερος σκοπός είναι η εκμετάλλευση των υπηρεσιών συστήματος μας.
Στις παλαιότερες εκδόσεις των Windows οι υπηρεσίες δεν μπορούσαν να τρέξουν με τα λιγότερα προνόμια . Στην πραγματικότητα οι υπηρεσίες των Windows συχνά τρέχουν σε λογαριασμούς με πολύ υψηλά επίπεδα πρόσβασης , όπως τον λογαριασμό **Local System** .
Υψηλά προνόμια σημαίνει συνεπώς ότι είναι επιτρεπτή η πρόσβαση σχεδόν σε όλους τους πόρους μέσα στο σύστημά μας .
Οι υπηρεσίες είναι πλέον εφοδιασμένες με μια ανά-υπηρεσία προσδιοριστική ταυτότητα **(SID-Security Identifier),** και σύμφωνα με αυτήν την ταυτότητα ελέγχεται και επιτρέπεται η είσοδος ή όχι σε διάφορες υπηρεσίες .
Η προσδιοριστική αυτή ταυτότητα ελέγχεται από εμάς είτε κατά την διάρκεια εγκατάστασης της υπηρεσίας μέσω του **ChangeServiceConfig2 API** ή με την χρήση της εντολής **SC.exe** στο CMD.
Οι υπηρεσίες στα Windows Vista , έχουν πια την δυνατότητα να τρέχουν σε λογαριασμούς με λιγότερα προνόμια όπως σε λογαριασμούς σαν τον **Local Service** ή τον λογαριασμό **Network Service**, σε αντίθεση με τον προνομιούχο **System account .**
Αναλυτικά ο λογαριασμός τοπικού συστήματος όπως ονομάζεται στα ελληνικά , έχει πολλά δικαιώματα και προνόμια όπως η δυνατότητα πρόσβασης σε σχεδόν οποιοδήποτε αντικείμενο και εάν επιθυμήσει ο χρήστης , ακόμη έχει την δυνατότητα πρόσβασης σε οποιοδήποτε προφίλ του χρήστη καθώς και σε ευαίσθητα σημεία του συστήματος όπως είναι τα κλειδιά μητρώου όπου οποιαδήποτε μετατροπή τους μπορεί να αποβεί καταστροφική για το σύστημα .
Περαιτέρω ,στις προηγούμενες εκδόσεις των Windows οι υπηρεσίες συστήματος έτρεχαν στην ίδια login session με αυτή της περιοχής τοπικής σύνδεσης του χρήστη δηλαδή την logged-in user session 0 , πράγμα που μπορεί να οδηγήσει σε μη επιθυμητή πρόσβαση κάποιας υπηρεσίας στον σύστημα μας .
Στα Windows Vista , η session 0 είναι πλέον διατηρημένη για αυτές τις υπηρεσίες συστήματος αλλά όλα τα άλλα logins γίνονται σε διαφορετικές συνόδους (sessions). Αυτός ο τρόπος

λειτουργίας προορίζεται να βοηθήσει μετριάζοντας μια κατηγορία από εκμεταλλεύσεις σε υπηρεσίες και μηνύματα που διαπερνάνε τα Windows γνωστά και ως **Shatter attacks**.
Οι χρήστες πολλές φορές δεν έχουν γνώση των υπηρεσιών που τρέχουν στα συστήματα τους και δεν μπορούν να αντιληφτούν ότι ορισμένες υπηρεσίες είναι ασφαλέστερο να είναι απενεργοποιημένες .
Υπάρχουν κάποιες υπηρεσίες οι οποίες χαρακτηρίζονται **επικίνδυνες** . Οι υπηρεσίες αυτές μπορούν να ξεκινήσουν αυτόματα κατά την εκκίνηση του υπολογιστή μας , μπορεί να σταματήσουν ή ακόμη να ξανά τεθούν σε λειτουργία χωρίς καμία ένδειξη στον χρήστη . Μπορούν ακόμη να εκτελούνται είτε στον λογαριασμό που είναι συνδεμένος ο χρήστης είτε σε διαφορετικό λογαριασμό . Γενικά αυτές οι υπηρεσίες έχουν μεγάλη ευελιξία , προσφέροντας έτσι μεγάλη διευκόλυνση στην ανάπτυξη ορισμένων κακόβουλων τύπων εφαρμογών.
Οι εμπειρογνώμονες της ασφάλειας δικτύου έχουν προ πολλού συνιστήσει ότι οι διαχειριστές θα πρέπει να απενεργοποιούν όλες τις περιττές υπηρεσίες για να μειώσουν έτσι τις περιπτώσεις εκμετάλλευσης τους .
Παρόλα αυτά υπάρχουν και ορισμένες υπηρεσίες οι οποίες δεν πρέπει να απενεργοποιηθούν , διότι είναι απαραίτητες να τρέχουν για την ορθή λειτουργία του υπολογιστή.
Οι υπηρεσίες ακόμη χρειάζονται ρητώς γραπτές άδειες ,για να μπορούν να γράψουν σε διάφορους πόρους ,και αυτές οι άδειες θα πρέπει με κάποιον τρόπο να διατηρούνται σε κάθε υπηρεσία.
Για να επιτευχθεί αυτό λοιπόν η υπηρεσία Hardening των Windows χρησιμοποιεί τα **γραπτώς περιορισμένα σημεία πρόσβασης (access token).** Μόνο στους πόρους , τους οποίους επιτρέπουμε εμείς να τροποποιήσει μια υπηρεσία ,δίνεται γραπτή πρόσβαση οποιαδήποτε άλλη μη αποδεκτή από εμάς προσπάθεια για να τροποποιηθεί οποιοσδήποτε άλλος πόρος θα αποτυγχάνει.
Τέλος οι υπηρεσίες έχουν επίσης προ-διαμορφωμένες πολιτικές Firewall, οι οποίες δίνουν σε αυτές μόνο τόσα προνόμια όσα είναι απαραίτητα για να λειτουργήσουν οι υπηρεσίες αυτές .
Ανεξάρτητα από τα λογισμικά οι διαχειριστές θα μπορούν να χρησιμοποιούν τον μηχανισμό του Service Hardening για να ¨σκληραίνουν¨ τις δικές τους υπηρεσίες .
Ως αποτέλεσμα των προηγουμένων , δηλαδή των υπηρεσιών που τρέχουν με περισσότερα από τα επιθυμητά και αναγκαία προνόμια , καθώς και υπηρεσίες που τρέχουν χωρίς να είναι απαραίτητες στον χρήστη, τα Windows παραμένουν πιο ευάλωτα στις επιθέσεις και οι χρήστες πιο ανυπεράσπιστοι να αντιμετωπίσουν τέτοιες καταστάσεις .
Στο σημείο αυτό είναι που εμφανίζεται ο όρος των Windows Service Hardening, αλλά προτού πάμε παρακάτω στην αναλυτική περιγραφή του μηχανισμού αυτού , καλό θα ήταν στο σημείο αυτό να εξηγήσουμε μερικούς ορισμούς τους οποίους θα βλέπουμε συχνά και θα μας απασχολήσουν στην συνέχεια.
Οι ορισμοί αυτοί είναι : **Επιθέσεις Επιφάνειας (attacks surface)**, **οι Υπηρεσίες Συστήματος (System Service)**, **η Προσδιοριστική Ταυτότητα Ασφάλειας (Security Identifier SID), η Λίστα Ελέγχου Πρόσβασης (ACL) , οι Shatter attacks και τέλος τα σημεία πρόσβασης (access token).**

7.3.1 Ορισμοί συσχετιζόμενοι με την υπηρεσία Windows Hardening

7.3.1.1 Τι είναι οι Επιθέσεις Επιφάνειας (attacks surface);

Οι επιθέσεις επιφάνειας ενός περιβάλλοντος λογισμικού αναφέρονται στις επιθέσεις που γίνονται στο πεδίο εκείνο του λειτουργικού το οποίο είναι διαθέσιμο για κάθε εφαρμογή των χρηστών και ιδιαίτερα των μη πιστοποιημένων χρηστών .

Το πεδίο αυτό συμπεριλαμβάνει , αλλά δεν περιορίζεται μόνο σε αυτά , τα ακόλουθα :

- Πεδία εισόδου χρήστη (User Input Fields).
- Πρωτόκολλα (Protocols).
- Προφίλ (Interfaces).
- Υπηρεσίες (Services).

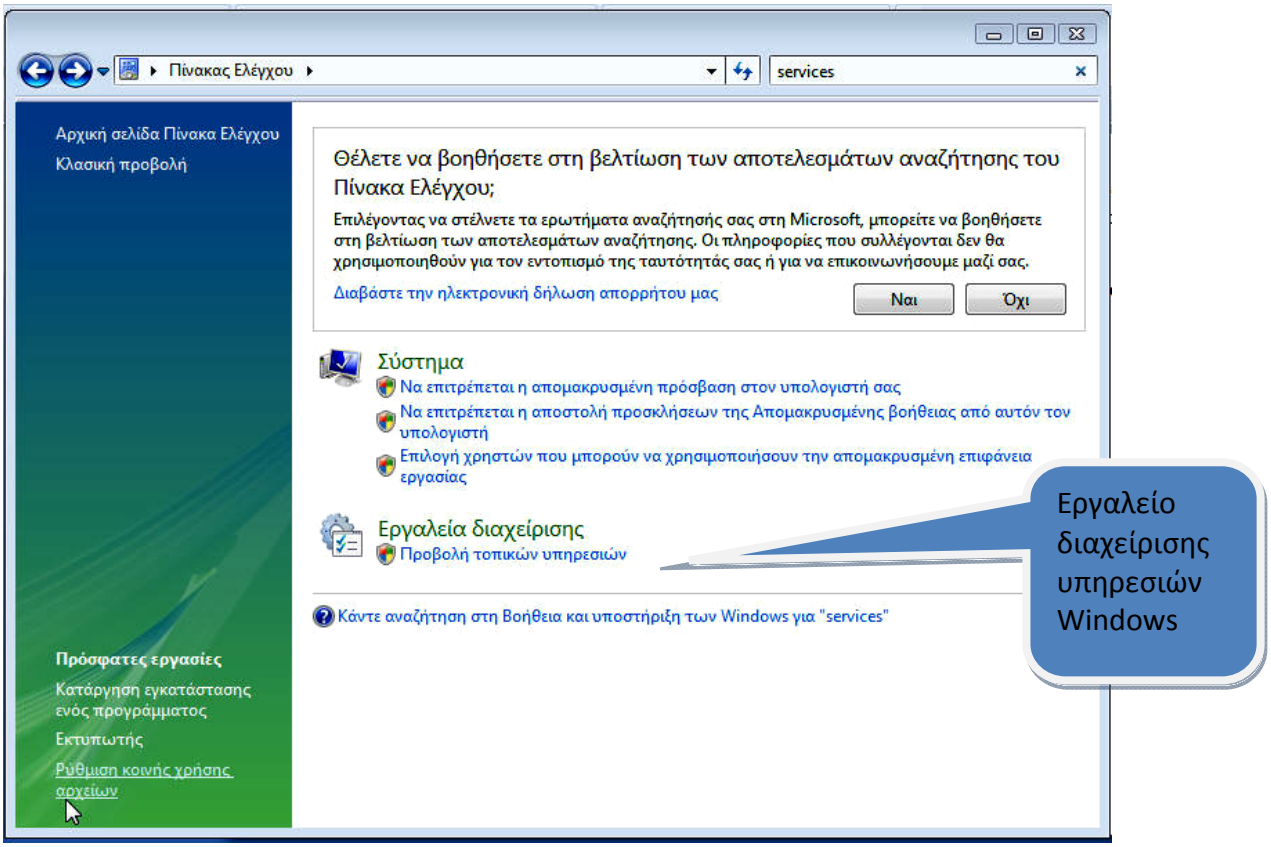
Μια προσέγγιση για να βελτιωθούν οι λεπτομέρειες ασφάλειας είναι να μειωθούν οι επιθέσεις επιφάνειας . Αυτό μπορεί να επιτευχθεί , κάνοντας εκείνο το κομμάτι του λειτουργικού μας πιο ανθεκτικό στις επιθέσεις .
Παρόλα αυτά αυτή η προσέγγιση μετριάζει σε μικρό βαθμό την ποσότητα των ζημιών που ένας καθορισμένος επιτιθέμενος μπορεί να προκαλέσει μόλις εντοπίσει μια ευπάθειά στο σύστημά μας .

7.3.1.2 Τι είναι οι Υπηρεσίες Συστήματος (Windows Services) και γιατί είναι ευάλωτες;

Στα λειτουργικά συστήματα της Microsoft Windows , η Υπηρεσία Windows είναι μια υπηρεσία μακράς χρήσης εκτελέσιμη οι οποία εκτελεί συγκεκριμένες λειτουργίες και η οποία είναι σχεδιασμένη να μην χρειάζεται την επέμβαση του χρήστη .
Οι υπηρεσίες Windows μπορούν να ρυθμιστούν να ξεκινούν είτε αυτόματα με την έναρξη του λειτουργικού συστήματος και να τρέχουν στο παρασκήνιο σε όλη την διάρκεια λειτουργίας των Windows , είτε χειροκίνητα όταν απαιτείται η χρήση τους .
Οι υπηρεσίες αυτές είναι παρόμοιες σε έννοια με το Unix Daemon.
Οι υπηρεσίες αυτές εμφανίζονται στον κατάλογο υπηρεσιών (στο Windows Task Manager) , συχνά με ένα username του συστήματος (System) ,της τοπικής υπηρεσίας (Local Service) ή τις υπηρεσίες δικτύου (Network Service).

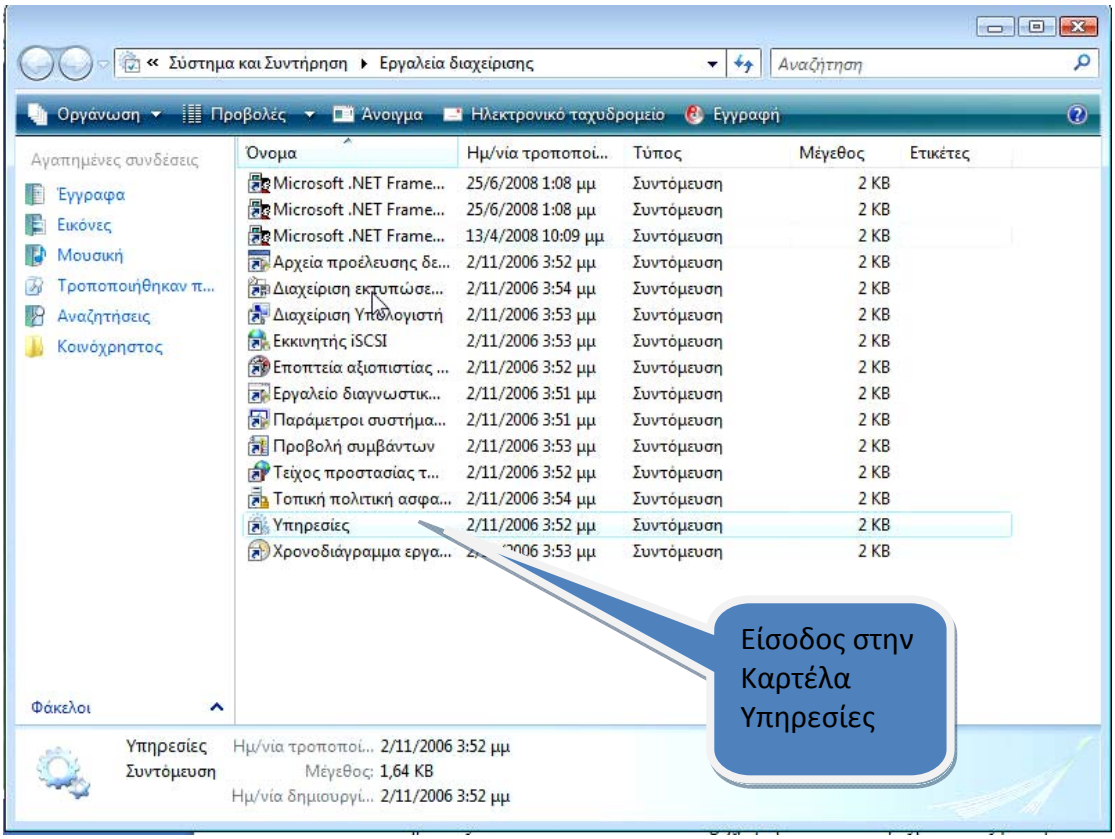
7.3.1.2.1 Πως γίνεται η διαχείριση των Υπηρεσιών Windows .

Μόλις μια υπηρεσία εγκατασταθεί , μπορεί να διαχειριστεί μέσω του παράθυρου ¨ **Υπηρεσίες** ¨ το οποίο μπορούμε να το βρούμε ακολουθώντας την διαδρομή **Πίνακας Ελέγχου** -> **Εργαλεία Διαχείρισης (Administrative Tools)** ή γράφοντας την εντολή ¨**Services.msc**¨ στην αναζήτηση η οποία βρίσκεται στο μενού έναρξης .
Η κονσόλα διαχείρισης των Υπηρεσιών παρέχει συνοπτική περιγραφή των λειτουργιών της κάθε υπηρεσίας και εμφανίζει επίσης το μονοπάτι στο οποίο η υπηρεσία εκτελείται , την παρούσα κατάσταση της , τον τύπο έναρξής της , τις εξαρτήσεις της και τέλος τον λογαριασμό στον οποίο αυτή τρέχει.

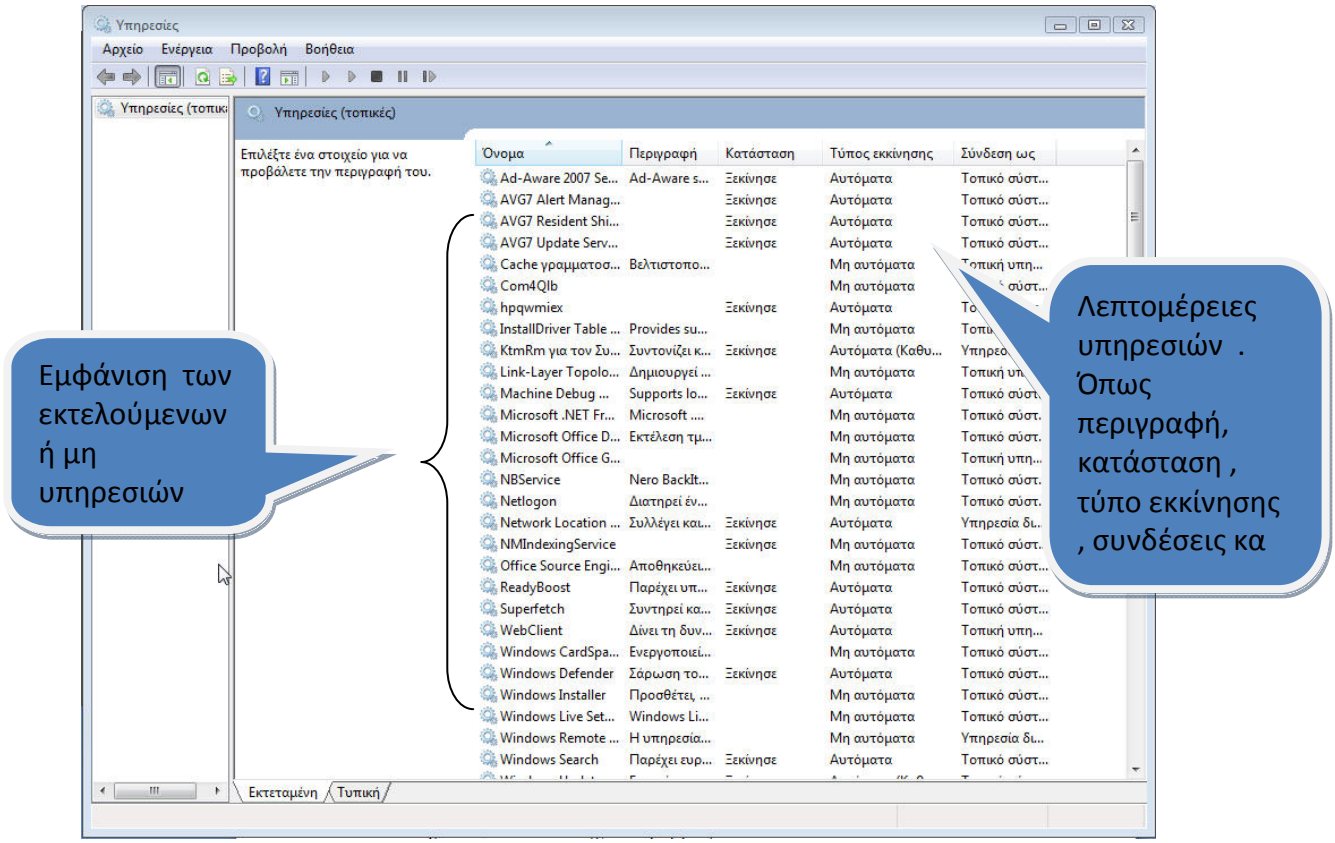


Εικόνα 85 : Καρτέλα Πίνακα Ελέγχου

Οι υπηρεσίες αυτές από την εγκατάστασή τους και μετά μπορούν να διαχειρίζονται μέσω της καρτέλας ¨**Services**¨ που βρίσκεται στον πίνακα ελέγχου .
Επιλέγοντας τα **Εργαλεία διαχείρισης** και στην συνέχεια επιλέγουμε **Υπηρεσίες** είτε γράφοντας στην αναζήτηση ¨**Services.msc**¨



Εικόνα 86 : Καρτέλα Εργαλεία Διαχείρισης.



Εικόνα 87 : Καρτέλα Υπηρεσίες.

Μέσω αυτής της καρτέλας οι χρήστες έχουν την δυνατότητα :

- Της εκκίνησης ,διακοπής ή επανεκκίνησης μιας υπηρεσίας.
- Καθορισμού των παραμέτρων της υπηρεσίας .
- Της αλλαγής του τύπου εκκίνησης , οποίος περιλαμβάνει της επιλογές Αυτόματη (Automatic), Χειροκίνητη (Manual) , Άτομα με ειδικές ανάγκες (Disabled).
  - Στην επιλογή Αυτόματη , η υπηρεσία ξεκινάει αυτόματα με την έναρξη του λειτουργικού συστήματος .
  - Στη επιλογή Χειροκίνητη , η υπηρεσία τίθεται σε λειτουργία μόνο όταν τις ζητηθεί από τον χρήστη ή από την εφαρμογή με την οποία είναι άμεσα συνδεδεμένη.
  - Στην τελευταία επιλογή , δηλαδή αυτή των Ατόμων με ειδικές ανάγκες , η υπηρεσία είναι πλήρως απενεργοποιημένη τόσο αυτή όσο και οι εξαρτήσεις να τρέχουν .
  - Αυτόματη- Καθυστερημένη (Automatic -Delayed) , είναι ένας νέος τύπος εκκίνησης ο οποίος παρουσιάζεται στα Windows Vista . Αυτός ο τύπος εκκίνησης ξεκινάει την υπηρεσία λίγο μετά την εκκίνηση του λειτουργικού συστήματος και αφού πρώτα αυτό έχει ολοκλήρωση την έναρξη όλων των αρχικών διαδικασιών . Με αυτόν τον τρόπο το σύστημα μας θα μπουτάρει πολύ γρηγορότερα .
- Της αλλαγής του λογαριασμού στον οποίο κάνει log on η υπηρεσία
- Την ρύθμιση επιλογών ανάκτησης σε περίπτωση αποτυχίας της υπηρεσίας
- Και τέλος την εξαγωγή της λίστας των υπηρεσιών σαν ένα κείμενο αρχείου ή CSV αρχείο .

Στα Windows XP και στα Windows Vista , εκτός από την καρτέλα διαχείρισης των υπηρεσιών , οι χρήστες μπορούν να διαχειριστούν τις υπηρεσίες χρησιμοποιώντας το **MSConfig** . Τέλος στα Windows Vista , μπορεί να χρησιμοποιηθεί ακόμη η **΄Εναρξη διαχείρισης εργασιών (Windows Task Manager)** για την επεξεργασία των ρυθμίσεων των υπηρεσιών .

7.3.1.3 Τι είναι Προσδιοριστική Ταυτότητα Ασφάλειας (Security Identifier SID);

Στο πλαίσιο της σειράς των λειτουργικών συστημάτων της Microsoft Windows NT , η προσδιοριστική ταυτότητα ασφάλειας συχνά αναφερόμενη και ως SID είναι ένα μοναδικό όνομα , (μια αλφαριθμητική σειρά χαρακτήρων string) η οποία ορίζεται από το Domain controller των Windows , κατά την διάρκεια του log-on της διαδικασίας και η οποία χρησιμοποιείται για να προσδιορίζει κάποιο αντικείμενο όπως πχ έναν user ή ένα group από χρήστες μέσα στο δίκτυο των NT/2000/2008 συστημάτων .
Αυτό το αναγνωριστικό είναι γνωστό και ως ¨**υπηρεσία ταυτότητας**¨ ή ¨**ανά υπηρεσία SID**¨ ή σε μερικά έγγραφα είναι γνωστό και απλά ως ¨**SID**¨ το οποίο όμως δε θα πρέπει να συγχέεται με την φράση ¨αναγνωριστικό ασφαλείας¨ το οποίο είναι και αυτό γνωστό ως SID και χρησιμοποιείται από τα Windows και το Active Directory . Η SID της υπηρεσίας απομόνωσης είναι μοναδική στην υπηρεσία αυτή και προέρχεται από το όνομα της υπηρεσίας.

7.3.1.3.1 Συνοπτική Περιγραφή –Χαρακτηριστικά του SID

Τα Windows επιτρέπουν ή αρνούνται την είσοδο καθώς και χορηγούν ή όχι προνόμια σε πόρους , βασιζόμενα στις Λίστες Πρόσβασης Ελέγχου (Access Control Lists - ACLs). Οι λίστες αυτές χρησιμοποιούν SIDs σε μεμονωμένους προσδιορισμένους χρήστες και σε ιδιότητες μελών group .
Όταν ένας χρήστης κάνει log – on σε έναν υπολογιστή ένα **σημείο πρόσβασης (access token)** , παράγεται το οποίο περιέχει του χρήστη και των group τα SIDs καθώς και το επίπεδο προνομίων του χρήστη .
Όταν ένας χρήστης ζητήσει πρόσβαση σε έναν πόρο το σημείο πρόσβασης ελέγχεται από την ACL για να επιτραπεί ή να απορριφθεί η συγκεκριμένη ενέργεια στο συγκεκριμένο αντικείμενο.
Οι SID είναι χρήσιμες για θέματα ανίχνευσης μηχανικών βλαβών με λογιστικούς ελέγχους ασφάλειας .
Ο σχηματισμός του SID έχει την ακόλουθη μορφή : **S-1-5-12-7623811015-3361044348-030300820-1013**
S- : Το string S δηλώνει ότι είναι SID.
1-: Το πρώτο ψηφίο δείχνει το επίπεδο αναθεώρησης .
5- :Δηλώνει την αξία της προσδιοριστικής αρχής .
12-7623811015-3361044348-030300820- : Είναι ο προσδιοριστής του Domain ή του τοπικού υπολογιστή.
1013- : Δηλώνει ένα συγγενικό ID (Relative ID RID).Οποιοδήποτε γκρουπ ή χρήστης ο οποίος δεν έχει δημιουργηθεί εξ ορισμού , έχουν συγγενικό ID 1000 ή μεγαλύτερο .
Πιθανές προσδιοριστικές τιμές αρχής είναι:
0 - Null Authority
1- World Authority.
2- Local Authority.
3- Creator Authority.
4- Non-unique Authority.
5- NT Authority.

7.3.1.3.2 ¨Γνωστές¨ Προσδιοριστικές Ταυτότητες Ασφάλειας.

Υπάρχει ένας αριθμός από προσδιοριστικές ταυτότητες ασφάλειας οι οποίες ορίζονται από το λειτουργικό σύστημα και οι οποίες διασφαλίζουν ότι κάποιοι συγκεκριμένοι λογαριασμοί του συστήματος πάντα θα αναγνωρίζονται .
Η Microsoft διατηρεί μια πλήρη λίστα αυτών των προσδιοριστών .

Πίνακας 7 : Περιγραφή των SIDs

SID	ΠΕΡΙΓΡΑΦΉ
S-1-5-18	Τοπικό σύστημα , ένας λογαριασμός υπηρεσίας ο οποίος χρησιμοποιείται από το λειτουργικό σύστημα
S-1-5-19	NT Authority , τοπική υπηρεσία
S-1-5-20	NT Authority , υπηρεσία δικτύου

S-1-5-21 Domain 500	Ένας λογαριασμός χρήστη για τον διαχειριστή του συστήματος . Εξ ορισμού είναι ο μοναδικός λογαριασμός χρήστη ο οποίος δίνει πλήρη έλεγχο του συστήματος
S-1-5-21 Domain 501	Λογαριασμός επισκέπτη χρήστη για άτομα που δεν έχουν συγκεκριμένους λογαριασμούς . Αυτοί οι λογαριασμοί χρηστών δεν απαιτούν password . Εξ ορισμού , ο λογαριασμός επισκέπτη είναι ανενεργός .
S-1-5-21 Domain 512	Domains Admins – Ένα παγκόσμιο γκρουπ του οποίου τα μέλη είναι εξουσιοδοτημένα να διαχειρίζονται τον τομέα. Εξ ορισμού το γκρουπ Domain Admins είναι μέλος των γκρουπ των Διαχειριστών , σε όλους τους υπολογιστές που συμμετέχουν στο τομέα συμπεριλαμβανομένου του τομέα ελέγχου . Τα Domain Admins είναι οι εξ ορισμού ιδιοκτήτες οποιουδήποτε αντικειμένου το οποίο δημιουργείται από οποιοδήποτε μέλος του γκρουπ.
S-1-5-21 Domain 513	Χρήστες τομέα
S-1-5-21 Domain 514	Επισκέπτες τομέα – Ένα παγκόσμιο γκρουπ το οποίο εξ ορισμού έχει ένα μόνο μέλος , τον λογαριασμό του τομέα του επισκέπτη built- in.

7.3.1.3.3 Το πρόβλημα των διπλών SIDs .

Το πρόβλημα με τα διπλά SIDs σε ένα Workgroup υπολογιστών οι οποίοι τρέχουν στα Windows NT/2K/XP/Vista , αφορά μόνο διαφορετικούς λογαριασμούς χρηστών που έχουν το ίδιο SID . Αυτό το φαινόμενο μπορεί να οδηγήσει σε αναπάντεχη πρόσβαση κοινόχρηστων αρχείων ή αποθηκευμένων αρχείων σε μετακινούμενα μέσα αποθήκευσης.
Εάν κάποια ACLs (Λίστες Πρόσβασης Ελέγχου) , είναι ρυθμισμένα σε κάποιο αρχείο , η πραγματική άδεια σχετίζεται με το SID του χρήστη . Εάν αυτό το SID χρήστη είναι διπλό σε κάποιο άλλο υπολογιστή (επειδή το SID του υπολογιστή είναι διπλό και επειδή το SID αυτό σχετίζεται με μια διαδοχική σειρά αριθμών), ο χρήστης ενός δεύτερου υπολογιστή που έχει το ίδιο SID μπορεί να έχει πρόσβαση στα αρχεία τα οποία ο χρήστης του πρώτου υπολογιστή τα έχει προστατευμένα.
Η αλήθεια είναι ότι όταν οι υπολογιστές που συμμετέχουν σε έναν τομέα (Active Directory ή NT domain, για παράδειγμα), κάθε υπολογιστής έχει έναν μοναδικό SID Domain ο οποίος ξανά ορίζεται κάθε φορά που ο υπολογιστής μπαίνει στο τομέα αυτό.
Κατά συνέπεια δεν υπάρχουν συνήθως πραγματικά προβλήματα με τα διπλά SID όταν οι υπολογιστές είναι μέλη ενός τομέα , ειδικά εάν οι λογαριασμοί τοπικοί χρηστών δεν χρησιμοποιούνται . Εάν οι λογαριασμοί των τοπικών χρηστών χρησιμοποιούνται είναι ένα πιθανό θέμα ασφάλειας το οποίο είναι το ίδιο με αυτό που περιγράψαμε παραπάνω όταν οι υπολογιστές είναι μέλη ενός Workgroup αλλά αυτό επηρεάζει μόνο τα αρχεία και τους πόρους που προστατεύονται από τοπικούς χρήστες και όχι από χρήστες του τομέα .
Με άλλα λόγια τα διπλά SIDs δεν αποτελούν συνήθως πρόβλημα στα συστήματα του Microsoft Windows .

7.3.1.4 Τι είναι Λίστες Πρόσβασης Ελέγχου (Access Control Lists -ACLs) ;

Στον τομέα της ασφάλειας των υπολογιστών η **Λίστα Πρόσβασης Ελέγχου (ACL)** είναι μια λίστα από άδειες οι οποίες είναι συνδεμένες σε κάποιο αντικείμενο. Η λίστα διευκρινίζει σε ποιον ή σε τι θα επιτρέπετε πρόσβαση στο αντικείμενο αυτό καθώς επίσης και ποιες διαδικασίες επιτρέπεται να εκτελούνται στο αντικείμενο.
Σε μια τυπική λίστα ACL κάθε είσοδο στην λίστα καθορίζει ένα θέμα και μια διαδικασία. Για παράδειγμα η είσοδος (Alice,delete) στην λίστα ACL για το αρχείο XYZ δίνει την άδεια στην Alice να διαγράψει το αρχείο XYZ.

7.3.1.4.1 Μοντέλα ασφάλειας βασισμένα στις ACLs λίστες .

Στο μοντέλο ασφάλειας το οποίο βασίζεται στον τρόπο λειτουργιάς των ACLs λιστών , όταν ένα θέμα ζητήσει να εκτελέσει μια λειτουργιά σε ένα αντικείμενο , το σύστημα πρώτα ελέγχει την λίστα για τις εφαρμόσιμες εισόδους με σκοπό να αποφασίσει εάν θα συνεχίσει με την διαδικασία ή όχι .
Βασικά ζητήματα στον καθορισμό οποιοδήποτε ACL – βασισμένου μοντέλου ασφάλειας είναι το πόσες λίστες πρόσβασης ελέγχου είναι προς επεξεργασία για κάθε αντικείμενο , το ποιος μπορεί να τροποποιήσει την λίστα του αντικειμένου και τι είδους αλλαγές επιτρέπονται;
Τα συστήματα τα οποία χρησιμοποιούν ACLs , ταξινομούνται σε 2 κατηγορίες : **Διακριτικές(Discretionary)** , και **Υποχρεωτικές (Mandatory).**

Ένα σύστημα λέγεται ότι διαθέτει διακριτικό έλεγχο πρόσβασης , όταν ο δημιουργός ή ο διοικητής ενός αντικειμένου μπορεί να έχει πλήρη έλεγχο πρόσβασης στο αντικείμενο συμπεριλαμβανομένου , για παράδειγμα , να μπορεί να αλλάζει την ACL του αντικειμένου και να χορηγεί πρόσβαση σε οποιοδήποτε άλλον και αν επιθυμεί.
Από την άλλη ένα σύστημα λέγεται ότι διαθέτει υποχρεωτικό έλεγχο πρόσβασης ,(γνωστό και ως μη-διακριτικό έλεγχο πρόσβασης), εάν του έχουν επιβληθεί , σε όλο το σύστημα περιορισμοί οι οποίοι δηλώνονται στην ACL .
Τα παραδοσιακά ACL συστήματα ορίζουν άδειες στους ατομικούς χρήστες , οι οποίες μπορούν να είναι δυσκίνητες σε ένα σύστημα με μεγάλο αριθμό χρηστών .
Σε μια πιο πρόσφατη προσέγγιση γνωστή με την ονομασία ¨Βασισμένος σε ρόλους έλεγχος πρόσβασης (role-based access control) ¨, οι άδειες ορίζονται σε ρόλους και οι ρόλοι ορίζονται στους χρήστες .

7.3.1.4.2 Σύστημα αρχείων ACLs

Στο σύστημα αρχείων ο προσδιορισμός των διαδικασιών των χρηστών είναι και ο αρχικός στόχος του ελέγχου UID. Η λίστα είναι μια δομή δεδομένων συνήθως ένας πίνακας ο οποίος περιέχει εισόδους που διευκρινίζουν του ατομικού χρήστη ή των χρηστών των γκρουπ τα δικαιώματα , σε συγκεκριμένα αντικείμενα συστήματος όπως πχ ένα πρόγραμμα , μια διαδικασία ή ένα αρχείο.
Αυτές οι είσοδοι είναι γνωστές και ως Είσοδοι Ελέγχου Πρόσβασης (ACE) στα Microsoft Windows, Open VMS, Linux και Mac OS X λειτουργικά συστήματα.
Κάθε προσβάσιμο αντικείμενο περιέχει έναν προσδιοριστή σε κάθε ACL .

Τα προνόμια ή οι άδειες καθορίζουν τα συγκεκριμένα δικαιώματα πρόσβασης , όπως το εάν ένας χρήστης θα έχει δικαίωμα να διαβάζει (read) , να γράφει (write) ή να εκτελεί (execute) ένα αντικείμενο.
Σε μερικές εφαρμογές οι ACE μπορούν να ελέγχουν το εάν ένας χρήστης ή ένα γκρουπ χρηστών μπορεί ή όχι να αλλάξει την ACL σε ένα αντικείμενο .
Η ACL είναι μια έννοια με πολλές διαφορετικές εφαρμογές σε διάφορα λειτουργικά συστήματα .Παρόλα αυτά υπάρχει ένα POSIX συγκεκριμένο . Το σχέδιο ασφάλειας POSIX .1e και .2c αποσύρθηκε όταν έγινε ξεκάθαρο ότι το πεδίο του ήταν πάρα πολύ ευρύ και η δουλειά η οποία του είχε ανατεθεί δεν θα ολοκληρωνόταν , παρόλα αυτά όμως τα καλώς αναπτυγμένα κομμάτια που καθορίζουν τις ACLs έχουν εφαρμοστεί ευρέως και είναι γνωστά ως ¨POSIX ACLs¨.
Οι διαχειριστές δικτύου θα πρέπει να βρουν το πώς θα απαγορεύουν τη μη επιθυμητή πρόσβαση στο δίκτυο ενώ ταυτόχρονα θα επιτρέπουν εσωτερικά στους χρήστες κατάλληλη πρόσβαση σε απαραίτητες υπηρεσίες.
Αν και τα εργαλεία συστήματος ασφάλειας όπως πχ τα password , ο εξοπλισμός επανάκλησης και οι φυσικές συσκευές ασφάλειας , είναι χρήσιμα παρόλα αυτά στερούνται συχνά την ευελιξία του βασικού φιλτραρίσματος κυκλοφορίας και των συγκεκριμένων ελέγχων που οι περισσότεροι διοικητές προτιμούν .
Για παράδειγμα, ο διαχειριστής δικτύου μπορεί να θελήσει α επιτρέψει στους χρήστες την πρόσβαση στοInternet αλλά να μην επιτρέπει την εξωτερική πρόσβαση Telnet των χρηστών στο LAN . Οι Routers , παρέχουν βασικές ικανότητες φιλτραρίσματος κυκλοφορίας όπως μπλοκάρισμα της κυκλοφορίας του Internet με την χρήση των ACLs .
Οι ACLs είναι όπως προαναφέραμε διαδοχικές λίστες οι οποίες περιέχουν δηλώσεις άδειας ή άρνησης οι οποίες ισχύουν σε συγκεκριμένες διευθύνσεις ή σε υψηλότερων επιπέδων πρωτόκολλα.
Στην ενότητα που ακολουθεί θα παρουσιάσουμε πως το τυποποιημένο εκτεταμένο ACL μπορεί να χρησιμοποιηθεί ως μέσο για να ελέγχει την κυκλοφορία των δικτύων και πως το ACL χρησιμοποιείται ως τμήμα μιας λύσης ασφάλειας για τα συστήματά μας.

7.3.1.4.3 Δικτύωση ACLs

Στην δικτύωση , με τον όρο ACL αναφερόμαστε σε μια λίστα από κανόνες που απαριθμούν τα ονόματα των πόρτων των υπηρεσιών ή (network) daemon (service ports ,or network daemon), οι οποίες είναι διαθέσιμες σε ένα host ή άλλη επιπέδου 3 συσκευή .Κάθε ένα ACL διαθέτει έναν κατάλογο από hosts και / ή δικτύων που επιτρέπεται να χρησιμοποιήσει η υπηρεσία. Και οι δυο οι μεμονωμένοι Serves όπως και οι Routers μπορούν να έχουν Network ACL.
Οι λίστες πρόσβασης ελέγχου μπορούν γενικά να τροποποιηθούν για να ελέγχουν ταυτόχρονα τόσο την εισερχόμενη όσο και την εξερχόμενη κίνηση και σε αυτό το πεδίο μοιάζουν με τα Firewalls.

7.1.3.5 Shatter attacks.

Στο κομμάτι αυτό θα εξηγήσουμε τον ορισμό της λέξης Shatter attack . Στο πεδίο των υπολογιστών η επίθεση shatter είναι μια τεχνική προγραμματισμού (shatter attack) που υιοθετείται από τους χάκερ και που εφαρμόζεται στα Microsoft Windows λειτουργικά συστήματα.
Η τεχνική αυτή μπορεί να χρησιμοποιηθεί για να παρακάμψει τους περιορισμούς ασφαλείας μεταξύ των διαδικασιών σε μια σύνοδο. Η shatter attack εκμεταλλεύεται μια ρωγμή σχεδίου στο σύστημα μηνυμάτων των Windows με την οποία ο αυθαίρετος κώδικας μπορεί να εισαχθεί σε

οποιαδήποτε άλλη εφαρμογή που τρέχει ή σε άλλες υπηρεσίες που βρίσκονται στην ίδια σύνοδο .Αυτή η επίθεση χρησιμοποιεί έναν βρόγχο μηνυμάτων , αυτό μπορεί να οδηγήσει σε μια κλιμακωμένη εκμετάλλευση προνομίων .

7.3.1.5 Συνοπτικά για την Shatter attack.

Οι επιθέσεις αυτής της μορφής έγιναν αντικείμενο έντονης συζήτησης τον Αύγουστο του 2002 μετά την έκδοση ενός εγγράφου του Chris Paget με τον τίτλο ¨Exploiting design flaws in the Win32 API for privilege escalation¨
Μέσω του εγγράφου αυτού δημιουργήθηκε ο όρος shatter attack εξηγώντας την διαδικασία μέσω της οποίας μια εφαρμογή μπορεί να εκτελέσει έναν αυθαίρετο κώδικα μέσα σε μια άλλη εφαρμογή . Αυτό μπορεί να συμβαίνει επειδή τα Windows επιτρέπουν μη προνομιούχες εφαρμογές να στέλνουν μηνύματα στο βρόγχο μηνυμάτων ή υψηλές προνομιούχες εφαρμογές και κάποια μηνύματα μπορούν να έχουν την διεύθυνση μιας αναδρομικής λειτουργίας στον χώρο διεύθυνσης της εφαρμογής σαν παράμετρός του .
Εάν ένας επιτιθέμενος κατορθώσει να τοποθετήσει το δικό του string μέσα στην μνήμη μιας υψηλά προνομιούχας εφαρμογής (το οποίο πετυχαίνεται με ένωση shell code σε ένα παράθυρο διαχείρισης ή χρησιμοποιώντας VirtualAllocEx και WriteProcessMemory) σε μια γνωστή τοποθεσία , μπορεί τότε να στείλει WM_TIMER μηνύματα με αναδρομικής λειτουργιάς παραμέτρους και να θέσει σε λειτουργία μια σειρά από παραταγμένα string.
Λίγες εβδομάδες μετά την δημοσιοποίηση αυτού του εγγράφου , η Microsoft απάντησε σημειώνοντας ότι ¨Το έγγραφο αυτό έχει δίκιο ότι αυτού του είδους οι επιθέσεις υπάρχουν και περιγράφει σωστά τις συνέπειές του …το σημείο στο οποίο το έγγραφο είναι λάθος είναι ότι ισχυρίζεται ότι οφείλεται σε μια ρωγμή των Windows. Στην πραγματικότητα η ρωγμή βρίσκεται σε συγκεκριμένη υψηλά προνομιούχα υπηρεσία . Εξ ορισμού όλες οι υπηρεσίες μέσα σε αλληλεπιδραστικές επιφάνειες εργασίας είναι υψηλό-προνομιούχες και μπορούν να επιβάλλουν αιτήσεις μεταξύ τους . Σαν αποτέλεσμα όλες οι υπηρεσίες σε αυτές τις επιφάνειες εργασίας έχουν ισοδύναμα υψηλόβαθμα προνόμια ¨ .

7.3.1.5.1 Λύσεις για την Shatter attack.

Τον Δεκέμβρη του 2002 , η Microsoft ζήτησε ένα patch για τα Windows NT 4.0, Windows 2000 και Windows XP . Το οποίο patch αποκλείει μερικές οδούς προς εκμετάλλευση. Αυτό ήταν μόνο μία μερική λύση παρόλα αυτά , καθώς το αποτύπωμα αυτό ήταν περιορισμένο στις υπηρεσίες συμπεριλαμβανομένων των Windows τα οποία θα μπορούσαν να τεθούν υπό εκμετάλλευση αν αυτή η τεχνική χρησιμοποιούτανε.
Η υπογεγραμμένη σχεδιασμένη ρωγμή ακόμη υπήρχε και θα μπορούσε ακόμη να χρησιμοποιηθεί , για να στοχεύσει άλλες εφαρμογές ή τρίτων κατασκευαστών υπηρεσίες .
Με τα Windows Vista , η Microsoft καταφέρνει να λύσει το πρόβλημα με δύο τρόπους :

- Η τοπικοί χρήστες δεν κάνουν log-in πλέον στο session 0 , κατά συνέπεια διαχωρίζονται ο βρόγχος μηνυμάτων των χρηστών που είναι συνδεμένων , από τις υψηλών προνομίων υπηρεσίες του συστήματος οι οποίες είναι φορτωμένες στο session 0.
- Ένα νέο χαρακτηριστικό με την ονομασία User Interface Privilege Isolation (UIPI) , εισήχθηκε , με το οποίο οι διαδικασίες μπορούν να είναι περισσότερο

προστατευμένες έναντι των shatter attacks αναθέτοντας ένα επίπεδο ακεραιότητας σε κάθε διαδικασίας .Προσπάθειες να σταλούν μηνύματα σε μια διαδικασία με ένα υψηλότερο επίπεδο ακεραιότητας θα αποτύχουν ακόμη και εάν και οι δύο διαδικασίες χρησιμοποιούνται από τον ίδιο χρήστη . Για παράδειγμα ο Internet Explorer7 χρησιμοποιεί το χαρακτηριστικό UIPI για να περιορίσει τις επεκτάσεις των συστατικών οι αποδόσεις αλληλεπιδρούν με το υπόλοιπο τμήμα του συστήματος .
Παρόλα αυτά δεν εμποδίζονται όλες οι αλληλεπιδράσεις ανάμεσα στις διαδικασίες σε διαφορετικά επίπεδα ακεραιότητας.

Οι τρόποι με τους οποίους οι σύνοδοι αλληλεπιδρούν έχει επανασχεδιαστεί στα Windows Vista και στα Windows Server 2008 . Έχουν προστεθεί προφυλάξεις ασφάλειας του λειτουργικού μας κατά των Shatter attacks.
Ο τοπικός χρήστης που έχει κάνει log-in κινήθηκε από την session 0 στην session 1 κατά συνέπεια διαχωρίζονται οι διαδικασίες του χρήστη από τις υπηρεσίες του συστήματος οι οποίες θα μπορούσαν να αποτελέσουν τρωτό σημείο του συστήματός μας .

Η υπηρεσία Αλληλεπιδραστικής Ανίχνευσης Υπηρεσιών στα Windows Server 2008 είναι μια υπηρεσία που δημιουργεί πτυχές αναδρομικής συμβατότητας , παρόλα που κάποια λογισμικά είχαν σχεδιαστεί με την υπόθεση ότι η υπηρεσία τρέχει στην ίδια σύνοδο με αυτήν του συνδεμένου χρήστη . Για να υποστηριχτεί αυτή η υπηρεσία τα Windows Vista και τα Windows Server 2008 περιλαμβάνουν την νέα αυτή υπηρεσία με την ονομασία υπηρεσία Αλληλεπιδραστικής Ανίχνευσης Υπηρεσιών η οποία καθιστά ικανή την πρόσβαση σε διαλόγους που δημιουργούνται από αλληλεπιδραστικές υπηρεσίες όταν αυτές εμφανίζονται .
Ο αλληλεπιδραστικός χρήστης εμφανίζεται σε ένα πλαίσιο διαλόγου και διαθέτει την ικανότητα να αλλάζει μετακινούμενος από την session 0 με σκοπό να έχει πρόσβαση στο πλαίσιο διαλόγου.

7.3.1.6 Σημείο πρόσβασης (Access Token).

Στα λειτουργικά συστήματα των Microsoft Windows , ένα σημείο πρόσβασης , περιλαμβάνει τις πληροφορίες ασφάλειας για μια logon session και προσδιορίζει τον χρήστη, το γκρουπ του χρήστη καθώς και τα προνόμια που διαθέτει ο χρήστης .

7.3.1.6.1 Περιγραφή του σημείου πρόσβασης .

Ένα σημείο πρόσβασης αναφέρεται ως ένα αντικείμενο που περιλαμβάνει τον περιγραφέα ασφάλειας μιας διαδικασίας . Ένας περιγραφέας ασφάλειας συνδέεται με μια διαδικασία και καθορίζει τον ιδιοκτήτη του αντικειμένου (σε αυτήν την περίπτωση την διαδικασία) και τα ACLs τα οποίο διευκρινίζουν πια επιτρεπόμενα δικαιώματα πρόσβασης θα χορηγηθούν και ποια όχι στον ιδιοκτήτη του αντικειμένου .
Εν τω μεταξύ καθώς ένα σημείο χρησιμοποιείται για να αντιπροσωπεύσει μόνο την πληροφορία ασφάλεια , αποτελεί τεχνικά ελεύθερο σχηματισμό και μπορεί να συμπεριλάβει οποιαδήποτε δεδομένα .
Το σημείο πρόσβασης χρησιμοποιείται από τα Windows όταν η διαδικασία ή η απειλή προσπαθεί να αλληλεπιδράσει με τα αντικείμενα των οποίων οι περιγραφείς ασφάλειας επιβάλλουν έλεγχο πρόσβασης (securable objects).

Ένα σημείο πρόσβασης αντιπροσωπεύεται από το αντικείμενο συστήματος του τύπου Token επειδή κάθε ένα σημείο είναι κανονικό αντικείμενο συστήματος η πρόσβασης στο ίδιο το σημείο μπορεί να ελέγχει με την βοήθεια ενός περιγραφέα ασφάλειας .Αλλά πρακτικά αυτό δεν πετυχαίνεται ποτέ .

Το σημείο πρόσβασης παράγεται από την υπηρεσία logon όταν ένας χρήστης εισέρχεται στο σύστημα και παρέχονται πιστοποιητικά από τον χρήστη τα οποία είναι αυθεντικοποιημένα ενάντια με την αυθεντικότητα της βάσης δεδομένων , διευκρινίζοντας τα δικαιώματα που διαθέτει ο χρήστης και εμπερικλείονται μέσα στον περιγραφέα ασφάλειας.
Το σημείο σχετίζεται με κάθε διαδικασία που δημιουργείται από την σύνοδο του χρήστη (διαδικασίες των οποίων κάτοχος είναι ο χρήστης).
Κάθε φορά που μια τέτοιου είδους διαδικασία εισέρχεται σε κάποιον πόρο ο οποίος έχει έλεγχο πρόσβασης σε λειτουργία , τα Windows κοιτάνε στον περιγραφέα ασφάλειας και συγκεκριμένα στο σημείο πρόσβασης , να δουν εάν ο χρήστης έχει στην κατοχή του την διαδικασία και αυτή έχει επιλεγεί να έχει πρόσβαση στην πληροφορία αυτήν και εάν όντως έχει τι είδους λειτουργίες (read, write/modify κτλ) ο χρήστης επιτρέπεται να κάνει.

Αν η λειτουργία πρόσβασης είναι επιτρεπόμενη στο πλαίσιο του χρήστη, τα Windows επιτρέπουν να συνεχιστεί η διαδικασία με την λειτουργία αλλιώς απαγορεύεται η πρόσβαση.

7.3.1.6.2 Τύποι σημείων πρόσβασης .

Υπάρχουν δύο τύποι σημείων πρόσβασης :

- **Αρχικό σημείο (Primary token):** Τα αρχικά σημεία έχουν την δυνατότητα μόνο να σχετίζονται με διαδικασίες , και αντιπροσωπεύουν το υποκείμενο ασφάλειας μιας διαδικασίας . Η δημιουργία των αρχικών σημείων και οι συσχετισμοί τους με τις διαδικασίες είναι και τα δύο προνομιούχες λειτουργίες , απαιτούν δύο διαφορετικά προνόμια στο όνομα των διαχωρισμών προνομίων . Το τυπικό σενάριο προβλέπει την υπηρεσία πιστοποίησης του σημείου , και μια υπηρεσία log-on που συσχετίζει αυτό με το κελί του λειτουργικού συστήματος του χρήστη. Οι διαδικασίες αρχικά κληρονομούν ένα αντίγραφο από το αρχικό σημείο της γονικής διαδικασίας. Η προσομοίωση σημείων μπορεί μόνο να συνδεθεί με τις απειλές και να αντιπροσωπεύσει ένα υποκείμενο ασφαλείας της client διαδικασίας .Η προσομοίωση σημείων συνήθως δημιουργούνται και συνδέονται με τις παροντικές απειλές σιωπηρά από IPC μηχανισμούς όπως πχ DCE RPC DDE και ονομαζόμενες PIPES.

- **Προσωποποίηση σημείου (Impersonation token):** Η προσωποποίηση σημείου είναι μια έννοια ασφάλειας , μοναδική στα Windows NT ,η οποία επιτρέπει προσωρινά σε μια εφαρμογή του server να είναι ο client από άποψη πρόσβασης , για να εξασφαλιστεί το αντικείμενο. Η προσωποποίησης έχει τρία δυνατά επίπεδα :

- Identification: Που επιτρέπει στον server να αποχτήσει την ταυτότητα του client.
- Impersonation: Που επιτρέπει τον server να εκτελέσει οποιαδήποτε πράξη πάνω στον client.
- Delegation: Η οποία είναι παρόμοια με την Impersonation αλλά επεκτείνεται και σε απομακρυσμένα συστήματα στα οποία ο server συνδέεται (μέσω της συντήρησης των πιστοποιητικών). Ο client μπορεί να επιλέξει το μεγαλύτερο επίπεδο προσωποποίησης (ενδεχομένως) που είναι διαθέσιμο στον server ως μια παράμετρο σύνδεσης .

Το Delegation και το Impersonation , είναι προνομιούχες λειτουργίες (το Impersonation αρχικά δεν ήταν αλλά η παλιά αδυναμία στην εφαρμογή του client APIs να αποτυγχάνει να απαγορεύει το default επίπεδο του ¨Identification¨ επιτρέποντας σε ένα μη προνομιούχο server να προσωποποιεί ένα ανεπιθύμητο προνομιούχο client , το απαιτούσε να γίνει).

7.3.1.6.3 Περιεχόμενα των σημείων πρόσβασης (Access Token).

Ένα σημείο αποτελείται από ποικίλα επίπεδα τα οποία περιλαμβάνονται αλλά δεν περιορίζονται :

- Έναν προσδιοριστή , τον προσδιοριστή της συσχετιζόμενης συνόδου logon . Η σύνοδος διατηρείται από την υπηρεσία επικύρωσης και επίκειται να προστεθούν σε αυτήν τα πακέτα αυθεντικότητας με μια συλλογή όλων των απαραίτητων πληροφοριών (πιστοποιητικά), στον χρήστη παρέχονται όλα αυτά με την είσοδο του στο σύστημα.

  Τα πιστοποιητικά χρησιμοποιούνται επίσης για την πρόσβαση σε απομακρυσμένα συστήματα , χωρίς να χρειάζεται ξανά από τον χρήστη η αυθεντικοποίηση (single sing -in), υπό τον όρο ότι όλα αυτά τα συστήματα χρησιμοποιούν και μοιράζονται μια αρχή επικύρωσης του προσδιοριστή χρήστη .Αυτό το πεδίο είναι το πιο σημαντικό και είναι αυστηρά read-only.
- Οι προσδιοριστές των ομάδων χρηστών (ή ακόμη πιο συγκεκριμένα των υποκειμένων) είναι μέρος και αυτοί του σημείου πρόσβασης . Η ομάδα των προσδιοριστών αυτών δεν μπορεί να διαγραφεί , αλλά μπορούν τεθούν εκτός λειτουργίας .Τα περισσότερα από αυτά τα γκρουπ είναι σχεδιασμένα ως σύνοδοι Id(session id) ,ένα πτητικό γκρουπ αντιπροσωπεύει την logon session ,επιτρέποντας την πρόσβαση του πτητικού αντικειμένου σχετιζόμενο με την session .

- Τα προσδιοριστικά ομάδας περιορισμού (παρέχονται προαιρετικά). Αυτό το επιπρόσθετο σύνολο των γκρουπ δεν χορηγεί επιπρόσθετες προσβάσεις αλλά περαιτέρω περιορίζει : η

πρόσβαση σε ένα αντικείμενο επιτρέπεται μόνο εάν επιτρέπεται η πρόσβαση ενός από αυτά τα γκρουπ . Τα περιορισμένα γκρουπ δεν μπορούν ούτε να διαγραφούν ούτε να τεθούν εκτός λειτουργίας . Τα περιορισμένα αυτά γκρουπ είναι ένα πρόσθετο χαρακτηριστικό και χρησιμοποιούνται στην εφαρμογή των **sandboxes .**

- Τα προνόμια , τα οποία είναι πρόσθετες δυνατότητες που διαθέτουν οι χρήστες . Τα περισσότερα προνόμια είναι εκτός λειτουργίας εξ ορισμού , για να εμποδιστεί η ζημιά από ασυνείδητα σε ασφάλεια προγράμματα . Στην έναρξη των Windows XP with SP2 και στον Windows Server 2003 τα προνόμια μπορούν μόνιμα να αφαιρεθούν από τα σημεία μέσω της εντολής **AdjustTokenPrivileges()** μαζί και οι ιδιότητες **SE_PRIVILEGE_REMOVED** .

7.3.2 Περιγραφή χαρακτηριστικών του Windows Service Hardening

Η υπηρεσία Windows Service Hardening έχει σχεδιαστεί με σκοπό να μετριάσει κάποιες από της απειλές που προαναφέραμε ελαχιστοποιώντας τις έλλειψης ασφαλείας των συστημάτων μας . Το Windows Service Hardening περιορίζει κρίσιμες υπηρεσίες των Windows από το να επιφέρουν ανεπιθύμητες αλλαγές στα αρχεία του συστήματος , στην registry , στο δίκτυο , καθώς και σε άλλες πηγές του συστήματος μας οι οποίες μπορούν να χρησιμοποιηθούν για να επιτρέψουν την εγκατάσταση κακόβουλου λογισμικού τόσο στον ίδιο υπολογιστή όσο και σε άλλους υπολογιστές του δικτύου .
Για παράδειγμα , η υπηρεσία απομακρυσμένης κλήσης (Remote Procedure Call), μπορεί να αντικατασταθεί χωρίς την άδεια μας από μια υπηρεσία αντικατάστασης αρχείων συστήματος ή ακόμη από μια υπηρεσία τροποποίησης του μητρώου του συστήματος . Και στις δύο περιπτώσεις θα βρεθούμε εκτεθειμένοι και η ασφάλεια μας θα έχει παραβιαστεί είτε με τον έναν είτε με τον άλλο τρόπο.
Στα προηγούμενα λειτουργικά συστήματα οι Windows υπηρεσίες αντιπροσώπευαν ένα μεγάλο ποσοστό των συνολικών επιθέσεων . Από την προοπτική της επίθεσης στην συνολική ποσότητα του ¨συνεχούς- ανοιχτού¨ κώδικα και αποτυπωμάτων του συστήματος μέχρι και τις επιθέσεις στα προνόμια επιπέδου του εν λόγω κώδικα .
Τα Windows Vista, περιορίζουν των αριθμό των υπηρεσιών που εκτελούνται και λειτουργούν από προεπιλογή ,περιορίζοντας έτσι σε κάποιο βαθμό των αριθμό των πιθανών επιθέσεων .
Τέλος στις μέρες μας πολλές υπηρεσίες από τρίτους κατασκευαστές τρέχουν σε λογαριασμούς με υψηλά προνόμια όπως ο Local System λογαριασμός , όπου οποιαδήποτε παράβαση ασφαλείας είναι μη αναστρέψιμη και μπορεί να οδηγήσει σε απεριόριστη βλάβη στο τοπικό μηχάνημα .

7.3.3 Ο σκοπός της Υπηρεσίας Hardening.

Αρχικά θα ισχυριστούμε ότι η υπηρεσία Hardening είναι σχεδιασμένη για να εμποδίσει τους επιτιθέμενους από το να θέσουν συμβιβασμούς στις υπηρεσίες .
Στην πραγματικότητα όμως δεν είναι αυτός ο πραγματικός λόγος λειτουργίας της υπηρεσίας αυτής .

Εκτός βέβαια από αυτήν την υπηρεσία υπάρχουν και άλλοι τέτοιου είδους μηχανισμοί ασφάλειας στα Vista , όπως πχ το Windows Firewall , το οποίο εκτελεί την λεγόμενη ¨εξωτερικού στρώματος ¨ προστασία.
Από την άλλη πάλι η υπηρεσία Hardening μειώνει τις πιθανότητες των κακόβουλων χρηστών από το να επηρεάζουν θέτοντας συμβιβασμούς σε οποιαδήποτε υπηρεσία προκαλώντας της έτσι ζημιά.
Θα αναφέρουμε ένα παράδειγμα μέσω του οποίου θα προσπαθήσουμε να προσδιορίσουμε καλύτερα τον σκοπό της λειτουργίας αυτής .
Σκεφτείτε σε ένα φυσικό πολύ-επίπεδο σχέδιο ασφάλειας , στο οποίο έχουμε οριοθετήσει έναν περιοριστικό φράχτη με ένα μεγάλο σκυλί στο εσωτερικό του με απώτερο σκοπό να κρατάμε τους διαρρηκτές μακριά από την ιδιοκτησία μας . Σε περίπτωση τώρα που οι διαρρήκτες αυτοί καταφέρουν να πλησιάσουν την πόρτα μας , εμείς εξοπλιζόμαστε με ισχυρές κλειδαριές στις πόρτες μας . Έστω τώρα ότι καταφέρουν να προσπεράσουν και τον φράχτη και το σκυλί ακόμη και τις ισχυρές κλειδαριές που διαθέτουμε , εμείς για να ενισχύσουμε την ασφάλεια μας θα θέσουμε ένα σύστημα συναγερμού σε λειτουργία με κύριο σκοπό να τους εκφοβίσουμε .
Παρόλο που το σύστημα αυτό του συναγερμού μπορεί να τους εκφοβίσει δεν είναι σε θέση όμως να τους εμποδίσει από το να εισβάλουν στην ιδιοκτησία μας ,αυτήν είναι κυρίως δουλειά του φράχτη , του σκυλιού και των ισχυρών κλειδαριών. Δουλειά του είναι να βρίσκεται εκεί έτσι ώστε σε περίπτωση που καταφέρουν αν αποφύγουν την εξωτερικού επιπέδου ασφάλεια , να τους περιορίσει έτσι ώστε να είναι λιγότερο ικανοί να προκαλέσουν ζημιές και να ξεφύγουν με τα πολύτιμα αγαθά μας.
Η υπηρεσία Hardening λοιπόν ταυτίζεται περισσότερο με το σύστημα συναγερμού , ένα εσωτερικού – επιπέδου στοιχείο μιας πολύ-επίπεδης στρατηγικής ασφάλειας .

7.3.4 Τι κάνει η Υπηρεσία Hardening.

Η υπηρεσία Hardening , όπως και ο μηχανισμός User Account Control έχει σχεδιαστεί για να διασφαλίζει ότι οι λογαριασμοί χρηστών ακόμη και οι λογαριασμοί διαχειριστών τρέχουν με τα λιγότερο δυνατά επίπεδα προνομίων , μειώνοντας έτσι οποιαδήποτε ζημιά θα προκαλείτο σε περίπτωση χρήσης τους .
Για παράδειγμα , πολλές υπηρεσίες οι οποίες έτρεχαν στον λογαριασμό Local System με τα επιθυμητά εκείνα υψηλά προνόμια , με την χρήση της υπηρεσίας Hardening τώρα είναι σε θέση να τρέχουν ακόμη και στους λογαριασμούς Network Service ή Local Service οι οποίοι διαθέτουν λιγότερα προνόμια .
Επιπλέον , προνόμια τα οποία οι υπηρεσίες δεν χρειάζονται για την λειτουργία τους όπως πχ το debugging , αφαιρούνται για να μειώσουν τις επιθέσεις επιφάνειας .
Υπηρεσίες οι οποίες τρέχουν σε λογαριασμούς με λιγότερα προνόμια συχνά αναφέρονται και ως ¨Περιορισμένες υπηρεσίες ¨.
Η λειτουργία των μηχανισμών ασφάλειας User Account Control και η Windows Service Hardening , αποτελούν παράδειγμα της αρχής της χρήσης των λιγότερων προνομίων .
Η οποία αρχή δηλώνει ότι κάθε χρήστης προγράμματος θα πρέπει να χρησιμοποιεί την λειτουργία αυτή και να θέτει εκτός λειτουργίας τα προνόμια τα οποία δε είναι απαραίτητα να λειτουργούν για να διεκπεραιώσουμε την δουλεία που επιθυμούμε .

7.3.5 Πως λειτουργεί το Windows Service Hardening.

Η υπηρεσίας Windows Service Hardening χρησιμοποιεί κάποιες μεθόδους για την αποφυγή όλων αυτών των καταστάσεων που προαναφέραμε καθώς και την επίτευξη του βασικού μας στόχου που είναι η ασφάλεια των προσωπικών μας δεδομένων .
Οι μέθοδοι που χρησιμοποιούνται για να επιτευχθούν αυτοί οι στόχοι είναι τέσσερεις και ακολουθεί λεπτομερής περιγραφή τους :

- Υπηρεσία απομόνωσης (Service Isolation),
- Όσο το δυνατών λιγότερα προνόμια (Least Privilege),
- Κλειστή η πρόσβαση στο δίκτυο (Restricted Network Access),
- Σύνοδος απομόνωσης (Session 0 Isolation).

Παρακάτω θα αναλύσουμε κάθε μια από αυτές τις περιπτώσεις εκτενέστερα .

7.3.5.1 Υπηρεσία Απομόνωσης

Στις προηγούμενες εκδόσεις των Windows , όταν μια υπηρεσία που επιθυμούσε πρόσβαση σε ένα αντικείμενο που απαιτείται υψηλό επίπεδο ασφάλειας , για να επιτευχθεί η διαδικασία αυτή ακολουθούσαμε μια από τις παρακάτω ενέργειες .

- Η ενέργεια εκτελούταν χρησιμοποιώντας ο χρήστης έναν λογαριασμό που διέθετε υψηλά επίπεδα δικαιωμάτων στο σύστημα . Ο Local System λογαριασμός για παράδειγμα προσφέρει αυτό το επίπεδο παρεχόμενων δικαιωμάτων και υπηρεσιών . Η χρήση αυτού του λογαριασμού , λοιπόν είναι μια λύση προκειμένου να εκτελεστεί η απαιτούμενη υπηρεσία , με αυτόν τον τρόπο όμως δημιουργούσαμε άσκοπα και επικίνδυνα και ευάλωτα ανοίγματα στο σύστημα μας με κίνδυνο της ασφάλεια σας για πιθανή επίθεση από κακόβουλα λογισμικά .

- Ένας εναλλακτικός τρόπος , για την αποφυγή των προηγούμενων καταστάσεων , ήταν η χρήση ενός λογαριασμού με λιγότερα προνόμια από τον Local System . Στο λογαριασμό όμως αυτόν θα έπρεπε να γίνει επαναρύθμιση των παραμέτρων ασφαλείας για το συγκεκριμένο αντικείμενο που επιθυμούσαμε πρόσβαση . Η μέθοδος αυτή αποτελούσε εφιάλτη για τον διαχειριστή του συστήματος όποιος θα έπρεπε να επαναριθμήσει κάθε μια υπηρεσία για κάθε ένα λογαριασμό ξεχωριστά. Φανταστείτε να πρέπει να δημιουργήσουμε ένα λογαριασμό υπηρεσίας και ξεχωριστά password για κάθε έναν λογαριασμό χρηστών ξεχωριστά . Μια διαδικασία χρονοβόρα η οποία εν τέλη δεν μας καθιστούσε και απολύτως ασφαλείς , καθώς εμφανίζοντας πάλι ευάλωτα σημεία με δυνατότητα επίθεσης από οποιοδήποτε ενδιαφερόμενο επιτιθέμενο απλά σε διαφορετικό επίπεδο από την προηγούμενη περίπτωση .

7.3.5.1.1 Εισαγωγή υπηρεσίας απομόνωσης .

Η υπηρεσία απομόνωσης , είναι μια μέθοδος η οποία μας βοηθάει να αντιμετωπίσουμε τις προηγούμενες αδιέξοδες και επικίνδυνες καταστάσεις . Με την βοήθεια της μεθόδου αυτής μια υπηρεσία των Windows Vista μπορεί να έχει πρόσβαση σε ένα απαιτούμενο αντικείμενο χωρίς να χρειάζεται να προσπερνά μέσα από διοικητικά μονοπάτια ή ακόμη χωρίς να χρειάζεται να χρησιμοποιεί έναν λογαριασμό διαχειριστή με υψηλού επιπέδου προνόμια όπως ο Local System λογαριασμός.
Η μέθοδος της απομόνωσης λειτουργεί με το να ασφαλίζει με ελεγχόμενη πρόσβαση ένα στόχο – αντικείμενο ,όπως παραδείγματος χάριν ένα κλειδί μητρώου , και να απαιτείται για την χρήση και επεξεργασία αυτού του αντικειμένου ένα αναγνωριστικό ασφαλείας .
.
Σε κάθε υπηρεσία , ορίζεται λοιπόν από μια SID η οποία έχει μια μοναδική τιμή . Όπως προαναφέραμε και πριν τα SIDs μας είναι εκ των προτέρων γνωστά λόγο των αναγνωριστικών ασφαλείας τα οποία ορίζονται σε όλους τους χρήστες και τα γκρουπ των Windows .
Αυτό λοιπόν το γνωστικό μοντέλο ελέγχου πρόσβασης των Windows μπορεί να χρησιμοποιηθεί επίσης για τον έλεγχο πρόσβασης των υπηρεσιών και να εφαρμοστεί στους πόρους του συστήματος .Κατά το ίδιο τρόπο που χρησιμοποιείται για τους απλούς λογαριασμούς αλλά και για τους λογαριασμούς των γκρουπ .
Με άλλα λόγια , οι λίστες ελέγχου πρόσβασης (ACLs) μπορούν τώρα να οριοθετούνται και για τις υπηρεσίες . Μια λίστα ελέγχου πρόσβασης (ACL) είναι ένα σύνολο από καταχωρήσεις ελέγχου πρόσβασης (ACEs). Κάθε πόρος διαθέτει κάποιον περιγραφέα ασφάλειας ο οποίος περιέχει τις ACLs οι οποίες είναι ορισμένες για αυτόν . Οι άδειες αυτές καθορίζουν το ποίος ή τι θα έχει πρόσβαση στο αντικείμενο αυτό , και όλες αυτές οι πληροφορίες αποθηκεύονται στην ACL.

Μόλις μια SID δημιουργηθεί και οριστεί προς χρήση από μια υπηρεσία , ενός αντικείμενου (παραδείγματος χάριν, ένα κλειδί μητρώου στο οποίο μια υπηρεσία χρειάζεται να γράψει κάποιες πληροφορίες) , ο κατάλογος ελέγχου πρόσβασης μπορεί να τροποποιηθεί και να περιλάβει το νέο SID , επιτρέποντας κατά συνέπεια στην υπηρεσία να έχει πρόσβαση στο αντικείμενο χωρίς να της δώσει παραπάνω δικαιώματα από τα απαραίτητα .
Με την χρήση λοιπόν των SIDs αντιμετωπίζεται το πρώτο πρόβλημα των ανεξέλεγκτων δικαιωμάτων που παρέχονται άθελα από κάποιους λογαριασμούς .
Τι γίνεται όμως σε περίπτωση που περιορίσουμε κάποια από αυτά τα SID .

7.3.5.1.2 Περιορισμένα SIDs

Σε περίπτωση που περιοριστεί κάποιο SID ακόμη και όταν αυτό χρησιμοποιείται από μια υπηρεσία , η υπηρεσία αυτή είναι σε θέση να εκτελείται και να έχει πρόσβαση σε άλλους επιθυμητούς πόρους επειδή η συμβολική διαδικασία των υπηρεσιών περιέχει επίσης SID για τον απολογισμό υπηρεσιών (i.e. , Local Service ή Network Service). Εαν μια υπηρεσία έχει δεχτεί κάποιους συμβιβασμούς, ένας πιθανός επιτιθέμενος μπορεί ακόμη να προκαλέσει κάποια

επιπρόσθετη ζημιά με το να εισαχτεί στους πόρους οι οποίοι δεν συσχετίζονται με την συγκεκριμένη υπηρεσία άμεσα αλλά οι οποίοι είναι προσβάσιμοι στον λογαριασμό Local Service.

Και σε αυτού του είδους την επίθεση τα Windows Vista προσπαθούν να μας βοηθήσουν και να μας προσφέρουν μια λύση . Προσπαθώντας λοιπόν να περιορίσουν τις πιθανές ζημιές που μπορούν να προκληθούν από συμβιβαζόμενες υπηρεσίες , τα Vista συνδυάζουν τα γραπτώς περιορισμένα σημεία και τα ανά-υπηρεσία SIDs για να καθιερώσουν κάποια συγκεκριμένα περιορισμένα SIDs για συγκεκριμένες υπηρεσίες .

Εάν μια υπηρεσία θέση σε λειτουργία κάποιο περιορισμένο SID , τότε αυτής της υπηρεσίας τα ανά-υπηρεσία SID τίθενται σε συνεργασία με την λίστα τόσο των κανονικών όσο και των περιορισμένων SID των γραπτός απαγορευμένων σημείων πρόσβασης των υπηρεσιών .
Με αυτόν τον τρόπο η υπηρεσία μπορεί να γράψει μόνο σε αντικείμενα τα οποία έχουν χορηγηθεί με πρόσβαση σε ένα από τα SIDs στην λίστα των περιορισμένων .
Ας δούμε ένα παράδειγμα.
Υποθέτουμε ότι μια υπηρεσία τρέχει στον λογαριασμό Local Service και επίσης διαθέτει ενεργή την SID της . Ωστόσο, η υπηρεσία αυτή έχει πρόσβαση τόσο στα αντικείμενα που έχει χορηγηθεί πρόσβαση λόγω της υπηρεσίας , όσο και σε όλα τα αντικείμενα στα οποία παρέχεται πρόσβαση λόγο του γεγονότος ότι η υπηρεσία βρίσκεται στον Local Service λογαριασμό.
Με το να θέτονται σε λειτουργία τα περιορισμένα SIDs , η υπηρεσία αυτή δεν έχει πλέον το δικαίωμα να γράφει σε κανένα αντικείμενο στο οποίο είχε πριν πρόσβαση λόγω του Local Service λογαριασμού .
Για ποιο λόγο ;
Διότι στα εν λόγω αντικείμενα δεν θα παρέχεται πια πρόσβαση εγγραφής στις ανά- υπηρεσίες SID της συγκεκριμένης υπηρεσίας .

7.3.5.2 Μέθοδος λιγότερων προνομίων

Η δεύτερη μέθοδος που χρησιμοποιεί ο μηχανισμός Service Hardening είναι αυτή των ¨Λιγότερων προνομίων¨.
Όπως προαναφέραμε πολλές υπηρεσίες τρέχουν εξ ορισμού στον ισχυρό λογαριασμό Local System. Ο Local System παρέχει τα απαραίτητα κλειδιά για κάθε πτυχή του συστήματός μας.
Ως εκ τούτου ο λογαριασμός αυτός καθώς και οι υπηρεσίες που τρέχουν σε αυτόν , αποτελούν ένα από τα πιο επιτυχημένα και δημοφιλή σημεία εκμετάλλευσης του συστήματος μας , από τους hackers. Καθώς αυτές οι υπηρεσίες μπορούν να τους προσφέρουν ευρύτατη και σε βάθος πρόσβαση στο σύστημα μας .
Προκειμένου , λοιπόν να προστατεύσουμε το σύστημά μας μια από τις καλύτερες λύσεις θα ήταν να τρέχουμε τις λειτουργίες μας χρησιμοποιώντας ένα λογαριασμό με τα λιγότερα δυνατά προνόμια. Τα οποία θα επαρκούν προκειμένου να μπορεί η υπηρεσία αν ολοκληρώσει τον στόχο της .

Παρόλο που τα Windows παρέχουν και άλλους λογαριασμούς οι οποίοι έχουν αισθητά λιγότερα προνόμια , ωστόσο ορισμένες υπηρεσίες για να λειτουργήσουν σωστά απαιτούν προνόμια που παρέχονται μόνο από τον Local System λογαριασμό.
Σύμφωνα με τις παλαιότερες εκδόσεις των Windows μόνο ο Local System λογαριασμός παρέχει εξουσιοδοτημένη πρόσβαση .
Σύμφωνα τώρα με τα Windows Vista οι υπηρεσίες που απαιτούν μόνο Local System λογαριασμού προνόμια μπορούν ακόμη να χρησιμοποιούν Local System λογαριασμό έχουν όμως ρυθμιστεί με τέτοιο τρόπο έτσι ώστε να τους χορηγούνται μόνο εκείνα τα προνόμια που είναι απαραίτητα για την λειτουργία της υπηρεσίας και τίποτα παραπάνω.
Ο Local System λογαριασμός δεν είναι ο μόνος λογαριασμός που μπορεί να χρησιμοποιήσει και να εκμεταλλευτεί το νέο αυτό χαρακτηριστικό .
Παρακάτω γίνεται μια αναφορά των λογαριασμών ή των τύπων λογαριασμών που μπορούν επίσης να χρησιμοποιήσουν αυτόν τον μηχανισμό των λιγότερων προνομίων.

- **Λογαριασμός Local Service**:

Ο λογαριασμός αυτός έχει τα λιγότερα προνόμια στον υπολογιστή μας και χρησιμοποιεί ανώνυμα πιστοποιητικά στο δίκτυο.
Αυτός ο λογαριασμός επίσης , έχει μειώσει τα προνόμια του και ενεργεί με έναν παρόμοιο τρόπο με αυτόν που λειτουργεί ο πιστοποιημένος τοπικός λογαριασμός χρήστη.
Η χρήση αυτού του λογαριασμού είναι χρήσιμη όταν ο Local System λογαριασμός παρέχει πάρα πολλά προνόμια και μεγάλη πρόσβαση στις υπηρεσίες οι οποίες παρόλα αυτά δεν χρειάζονται τόσο εις βάθος πρόσβαση στο σύστημα .

- **Λογαριασμός Network Service:**

Αυτός ο λογαριασμός είναι παρόμοιος με τον Local Service λογαριασμό μόνο που σε αυτόν τον λογαριασμό παρέχονται λιγότερα προνόμια από αυτά του Local Service . Το επόμενο σημείο στο οποίο διαφέρει από τον Local Service λογαριασμό είναι στην περίπτωση κατά την οποία μια υπηρεσία χρειάζεται πρόσβαση σε έναν απομακρυσμένο πόρο .
Γνωρίζουμε από προηγουμένως ότι ο Local Service λογαριασμό παρέχει ανώνυμα πιστοποιητικά προκειμένου να εισέρθει σε κάποιον απομακρυσμένο πόρο . Στον Network Service λογαριασμό οι προσβάσεις σε απομακρυσμένους πόρους επιτυγχάνονται χρησιμοποιώντας τα πιστοποιητικά του λογαριασμού του υπολογιστή τα οποία δεν είναι ανώνυμα .

- **Λογαριασμός Domain :**

Οι λογαριασμοί χρήστη δημιουργούνται στο Active Directory και Directory Domain .

- **Τοπικός λογαριασμός:**

Και τέλος έχουμε τους τοπικούς λογαριασμούς ή αλλιώς Local Account . Οι οποίοι δημιουργούνται στον τοπικό υπολογιστή.

Στα Windows Vista όταν μια υπηρεσία ξεκινήσει να λειτουργεί , η υπηρεσία απαιτεί συγκεκριμένα προνόμια . Όχι όλα τα προνόμια που παρέχονται από τον Local System λογαριασμό.

Προνόμια τα οποία δεν απαιτούνται για συγκεκριμένο σκοπό , με κάποιο τρόπο αφαιρούνται από το σημείο πρόσβασης της υπηρεσίας .
Εάν μια υπηρεσία τώρα δεν έχει εξ ορισμού οριοθετηθεί με όλα αυτά τα νέα χαρακτηριστικά ασφάλειας τότε σε αυτήν την υπηρεσία ορίζονται όλα τα δικαιώματα που χορηγούνται από τον Local System λογαριασμό.
Αυτό βοηθάει να διατηρηθεί προς τα πίσω συμβατότητα με παλαιότερες υπηρεσίες .
Για τις υπηρεσίες κοινής χρήσης τώρα , σε διαδικασίες που παίρνουν μέρος σε γκρουπ , οριοθετούνται τα δικαιώματα εκείνα που ζητούνται από κάθε διαδικασία ξεχωριστά .
Είναι σημαντικό να σημειωθεί ότι αυτή η αρχή των λιγότερων προνομίων δεν περιορίζουν την ικανότητα των hackers να εκμεταλλεύονται τα ψεγάδια των εκάστοτε υπηρεσιών .
Παρόλα αυτά περιορίζουν τις ζημιές οι οποίες μπορούν να προκληθούν από τα κακόβουλα λογισμικά τα οποία έχουν καταφέρει να δημιουργήσουν ένα επιτυχημένο ρήγμα , και έχουν καταφέρει να προσπεράσουν τους άλλους μηχανισμούς ασφάλειας μας.

7.3.5.3 Μέθοδος περιορισμένης πρόσβασης στο δίκτυο

Η τρίτη μέθοδο του Service Hardening είναι η μέθοδος περιορισμένης πρόσβασης στο δίκτυο .
Με τα χρόνια οι υπηρεσίες που τρέχουν στα Windows εξαρτώνται όλο και περισσότερο μεταξύ τους , και έχουν ανάγκη όλο και περισσότερο να έχουν πρόσβαση στο Ιντερνέτ , τέλος είναι πλέον απαραίτητο να είναι προσβάσιμες από άλλους υπολογιστές .
Οι υπηρεσίες αυτές οι οποίες έχουν να κάνουν με το δίκτυο , λόγο τις ιδιότητας τους αυτής είναι περισσότερο ευάλωτες από ότι οι υπόλοιπες ακόμη το γεγονός ότι οι υπηρεσίες αυτές περιμένουν τις απομακρυσμένες συνδέσεις προκειμένου να δουλέψουν τις καθιστά περισσότερο προσβάσιμες σε κακόβουλες δραστηριότητες.

Η μέθοδος λοιπόν αυτή σχετίζεται άμεσα με το Firewall των Windows καθώς και με τις ρυθμίσεις που ενσωματώνονται μέσα σε αυτό .
Ένα ακόμη λοιπόν θετικό και αξιοσημείωτο για να αναφορά σημείο είναι ότι οι πολιτικές του Network Firewall , οι οποίες μπορούν και αυτές επίσης να εφαρμοστούν σε υπηρεσίες με την εκάστοτε πολιτική να συνδέεται με το SID της υπηρεσίας .
Με αυτόν τον τρόπο μπορούμε να απαγορέψουμε σε διάφορες υπηρεσίες να έχουν πρόσβαση στο δίκτυο όταν αυτές επιχειρήσουν να συνδεθούν με τρόπο μη αποδεκτός από εμάς .
Στο Firewall των Vista είναι ενσωματωμένο το νέο αυτό χαρακτηριστικό Service Hardening.
Συγκεκριμένοι κανόνες έχουν οριστεί στην πλατφόρμα του Service Hardening , ως προς τον τρόπο με τον οποίο μια συγκεκριμένη υπηρεσία θα έχει πρόσβαση στο δίκτυο , στην Registry, ακόμη και στα αρχεία του συστήματος .

Το Firewall επιβάλλει αυτούς τους κανόνες και μπλοκάρει οποιαδήποτε άλλη κίνηση η οποία τους παραβιάζει .
Σε αντίθεση τώρα με το Firewall των XP , το Firewall των Vista μπορεί να εφαρμόσει ταυτόχρονα τόσο εισερχόμενους όσο και εξερχόμενους κανόνες.
Στα Windows Vista μπορεί ακόμη ένας προγραμματιστής να απαγορέψει την πρόσβαση σε μια υπηρεσία είτε μέσω της TCP/UDP πόρτας , του πρωτοκόλλου ή ακόμη και μέσω της κατεύθυνσης της κίνησης του δικτύου που ρέει .
Όταν περιορισμοί τέτοιου είδους έχουν τεθεί σε λειτουργία , οποιεσδήποτε προσπάθειες πρόσβασης στις υπηρεσίες χρησιμοποιώντας άλλες μη επιτρεπτές μεθόδους μπλοκάρονται προστατεύοντας την εν λόγω υπηρεσία από κάποια επίθεση φορέα.

Οι υπηρεσίες Windows Vista μπορούν να ρυθμιστούν ακόμη έτσι ώστε να μην τους επιτρέπεται η πρόσβασης τους στο δίκτυο , και σε αυτήν την περίπτωση οι υπηρεσίες θα προστατεύονται κατά έναν βαθμό καθώς ούτε αυτές θα συνδέονται στο δίκτυο άλλα ούτε οποιοδήποτε κακόβουλο λογισμικό δεν θα μπορεί να συνδεθεί μαζί τους παραβιάζοντας τες έτσι και από μακριά .
Με αυτόν τον τρόπο συγκεκριμένες υπηρεσίες μπορούν να περιοριστούν έτσι ώστε να μην μπορούν να κάνουν οποιαδήποτε αλλαγή είτε στην Registry είτε στα αρχεία του συστήματος είτε στο δίκτυο είτε και αλλού.
Ακόμη μπορεί μέσω αυτής της τεχνικής μια συγκεκριμένη υπηρεσία να περιοριστεί έτσι ώστε να μην μπορεί να γράψει σε μια μόνο συγκεκριμένη περιοχή των αρχείων του συστήματος ή ακόμη να μην μπορεί να έχει καμία εξωτερική σύνδεση δικτύου .
Στις υπηρεσίες μπορεί να απαγορευτεί η ικανότητα να μπορούν να κάνουν αλλαγές στις ρυθμίσεις διαμόρφωσης και να μην μπορούν να εκτελούν ενέργειες οι οποίες μπορούν να προκαλέσουν ζημιά στο σύστημα μας .
Σε κάθε υπηρεσία , η οποία συμπεριλαμβάνεται στα Windows Vista, έχει εξ ορισμού οριστεί ένα Service Hardening προφίλ , το οποίο καθορίζει τι επιτρέπεται και τι όχι να κάνει η συγκεκριμένη υπηρεσία . Στο σημείο αυτό το SCM (Service Control Manager) εκχωρεί πια τα προνόμια εκείνα που χρειάζονται και μόνο αυτά.
Έτσι με αυτόν τον τρόπο δεν απαιτείται κάποια επιπλέον ρύθμιση ή κάποια διοικητική επιβάρυνση.

7.3.5.4 Μέθοδος συνόδου απομόνωσης 0 (Session 0 Isolation)

Τέλος έχουμε την μέθοδο απομόνωσης συνόδου 0 . Για την μέθοδο αυτή , η βασική ιδέα είναι ότι χρησιμοποιούνται τα Windows Vista ως μια επιφάνεια εργασίας , και όχι ως ένας εξυπηρετητής (server) υπολογιστών απομακρυσμένων χρηστών .
Σύμφωνα με το λειτουργικό σύστημα των Windows XP , όταν ένας χρήστης συνδεθεί στο σύστημα όλες οι υπηρεσίες και οι εφαρμογές που εκτελούνται στο σύστημα αυτό , θεωρείται ότι εκτελούνται όλες μαζί σε ένα κομμάτι του συστήματος που ονομάζεται σύνοδος 0 (session 0) .
Σε περίπτωση τώρα που ενεργοποιηθεί η γρήγορη εναλλαγή χρηστών στα Windows XP , οι εφαρμογές του αρχικού χρήστη , αυτού δηλαδή που έχει συνδεθεί πρώτος στο σύστημα , θα οριστεί ότι λειτουργούν στην session 0 , μαζί και με όλες τις υπηρεσίες του συστήματος που εκτελούνται εκείνη την στιγμή.

Οι επιπλέον χρήστες που θα συνδεθούν στην συνέχεια στο σύστημα μέσω της γρήγορης εναλλαγής χρηστών καθώς και οι επιπλέον εφαρμογές των χρηστών που θα τεθούν σε λειτουργία θα τρέχουν μέσα σε μια νέα σύνοδο και όχι αυτήν την συνόδου 0.
Έτσι του δεύτερου χρήστη κατά σειρά, οι εφαρμογές θα τρέχουν στην σύνοδο 1 (session 1) , του τρίτου χρήστη στην σύνοδο 2 (session 2) κοκ
Ωστόσο άσχετα από το πόσοι χρήστες θα έχουν εισαχθεί στο σύστημα , όλες οι υπηρεσίες των Windows όπως και οι αρχικές εφαρμογές αυτές δηλαδή του αρχικού χρήστη , θα συνεχίζουν να εκτελούνται στην σύνοδο 0 (session 0).

Το να αναμιγνύουμε υπηρεσίες , πολλές από τις οποίες τρέχουν με ιδιαίτερα μεγάλα προνόμια , με τις εφαρμογές του χρήστη είναι ένα γεγονός που μπορεί να δημιουργήσει σημαντικά ζητήματα ασφάλειας .
Για παράδειγμα, εάν μια εφαρμογή η οποία είναι κακώς γραμμένη , πέσει θύμα εκμετάλλευσης ή εάν αυτή η εφαρμογή τρέχει στην ίδια σύνοδο με άλλες υπηρεσίες οι υπηρεσίες αυτές μπορούν να επηρεαστούν και να δεχτούν συμβιβασμούς και είναι το ίδιο τρωτές με την υπηρεσία- θύμα .

Εάν όμως οι υπηρεσίες αυτές λειτουργούσαν σε διαφορετικά κομμάτια δεν θα επηρεαζόντουσαν μεταξύ τους και θα ήταν έτσι περισσότερο ασφαλείς .

Με σκοπό λοιπόν . την καταπολέμηση αυτής της δυνητικής απειλής τα Windows Vista δεν επιτρέπουν σε καμία εφαρμογή του χρήστη να τρέχει στην σύνοδο 0 , για τον λόγο ότι όπως προαναφέραμε σε αυτήν βρίσκονται οι πολύ σημαντικές υπηρεσίες των Windows .
Όλες οι άλλες εφαρμογές ρυθμίζονται απλά να τρέχουν είτε στην σύνοδο 1 , είτε σε υψηλότερες συνόδους.
Μόνο οι υπηρεσίες συστήματος και οι άλλες μη συσχετιζόμενες με τις εφαρμογές του χρήστη υπηρεσίες , τρέχουν στην σύνοδο 0 .
Κατά συνέπεια επιτυγχάνεται απομόνωση μεταξύ των υπηρεσιών και των εφαρμογών χρήστη.

7.3.6 Windows Service Hardening Στην πράξη.

Στο κομμάτι αυτό θα παρουσιάσουμε βήμα βήμα τις ενέργειες που θα πρέπει να εκτελέσουμε προκειμένου να επιτύχουμε μεθόδους σκλήρυνσης που αναφέραμε παραπάνω.

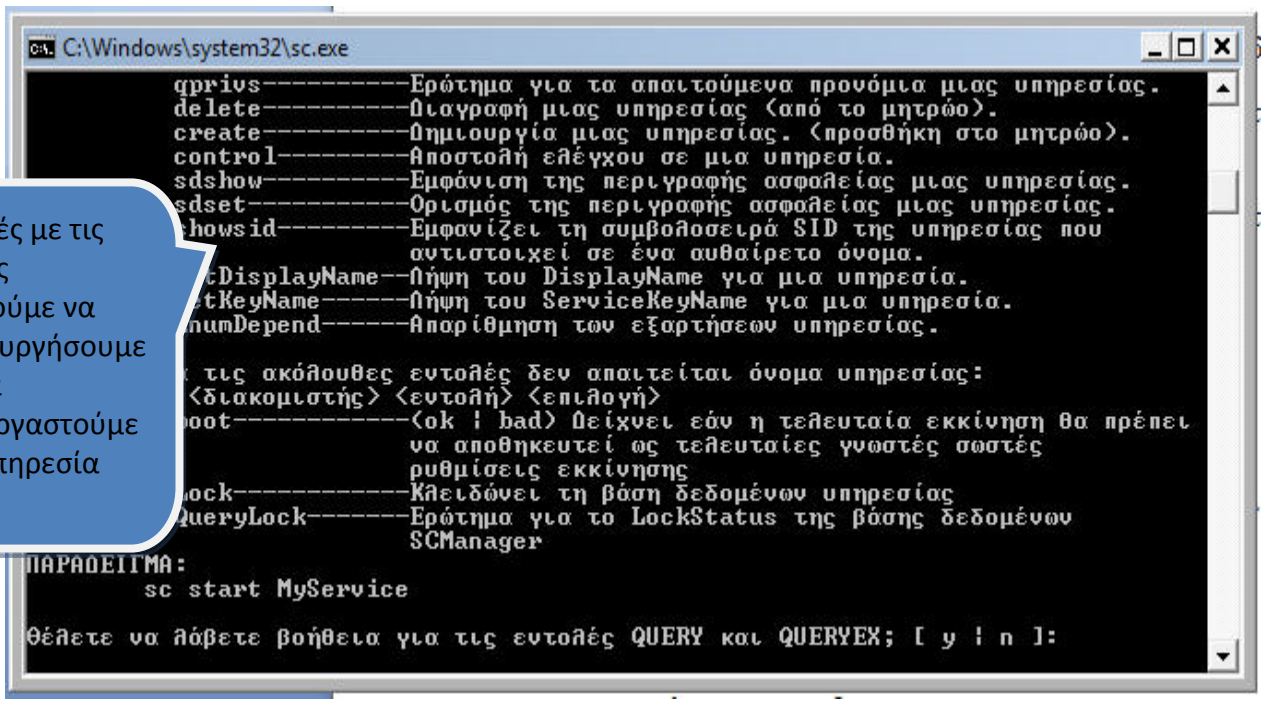
7.3.6.1 Ενεργοποίηση των SIDs

Αρχικά θα ασχοληθούμε με τα βήματα που απαιτούνται προκειμένου να ενεργοποιηθούν οι απενεργοποιηθούν τα SIDs των υπηρεσιών .
Το ανά – υπηρεσία SID δημιουργεί , στην ουσία , μια ταυτότητα για κάθε υπηρεσία η οποία επιτρέπει έλεγχο πρόσβασης χρησιμοποιώντας το ήδη υπάρχον μοντέλο του ελέγχου πρόσβασης των Windows.

Οι υπηρεσίες είναι σε θέση πλέον να κάνουν αιτήσεις χρήσης, στους μοναδικούς καταλόγους πρόσβασης ελέγχου (ACL´s), για πόρους οι οποίοι είναι ιδιωτικοί εμποδίζοντας έτσι άλλες υπηρεσίες όπως πχ και από τον χρήστη να έχει πρόσβαση στους πόρους αυτούς.
Οι ανά- υπηρεσίες SIDs μπορούν ακόμη να ρυθμίζονται είτε κατά την διάρκεια της εγκατάστασης της υπηρεσίας μέσω του **ChangeServiceConfig2 API** ή με την χρήση διάφορων εντολών στο cmd στο οποίο έχουμε προηγουμένως την εντολή **SC.EXE** χρησιμοποιώντας ακόμη τον προσδιοριστικό τύπο ασφάλειας της υπηρεσίας (γνωστό και ως SidType).

Οι προσδιοριστικοί αυτοί τύποι της ασφάλεια μπορεί να είναι οι ακόλουθοι : user , group, domain, alias, well_know group, deleted_account, invalid, computer .

Εκτελώντας λοιπόν την εντολή sc.exe μας εμφανίζεται το ακόλουθο παράθυρο το οποίο μας βοηθάει παρέχοντας μας τις απαραίτητες εντολές που ίσως χρειαστεί να εφαρμόσουμε προκειμένου να ρυθμίσουμε οποιεσδήποτε παραμέτρους σε οποιαδήποτε υπηρεσία και αν επιθυμούμε .



Εικόνα 88: Παράθυρο εντολής sc.exe

Υπάρχουν τρείς πιθανές τιμές για κάθε υπηρεσία :

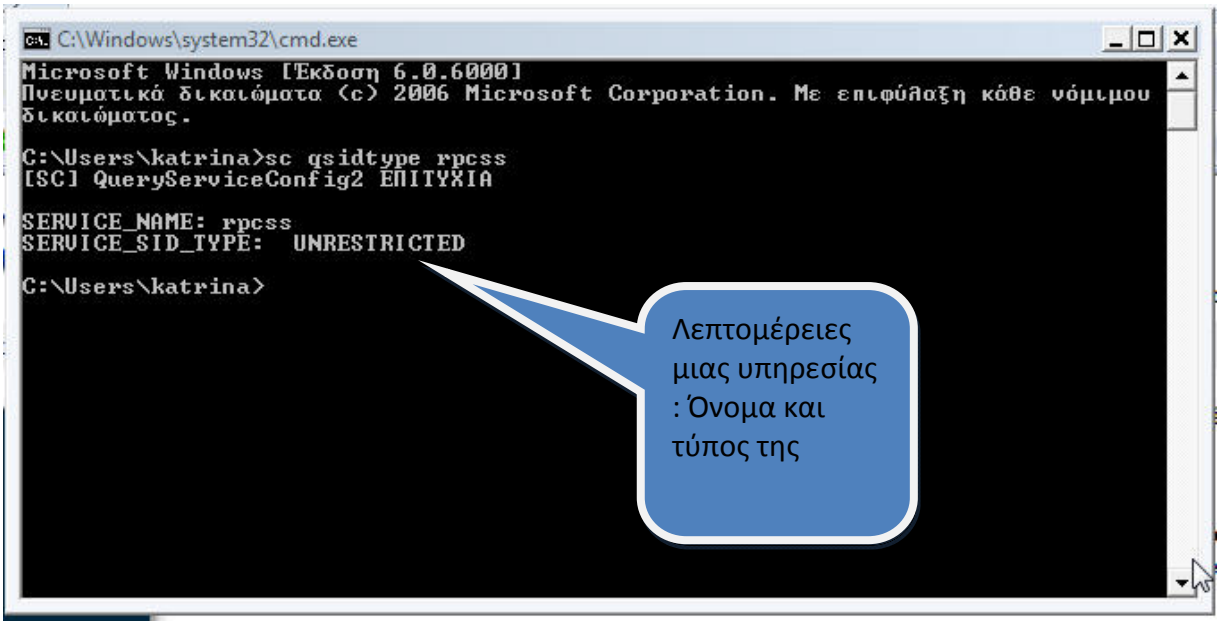
- **None (0x0),** η οποία δηλώνει ότι η υπηρεσία δεν διαθέτει προσωπική SID .Αυτοί είναι και οι default ρύθμιση κάθε υπηρεσίας.
- **Η απεριόριστη (0x1),** η οποία δηλώνει ότι η υπηρεσία διαθέτει προσωπική SID
- **Περιορισμένη (0x3),** η οποία δηλώνει ότι η υπηρεσία διαθέτει προσωπική SID και γραπτό περιορισμένο σημείο .

Έστω τώρα ότι επιθυμούμε να δημιουργήσουμε εμείς υπηρεσία . Τα βήματα που ακολουθούμε είναι τα εξής :

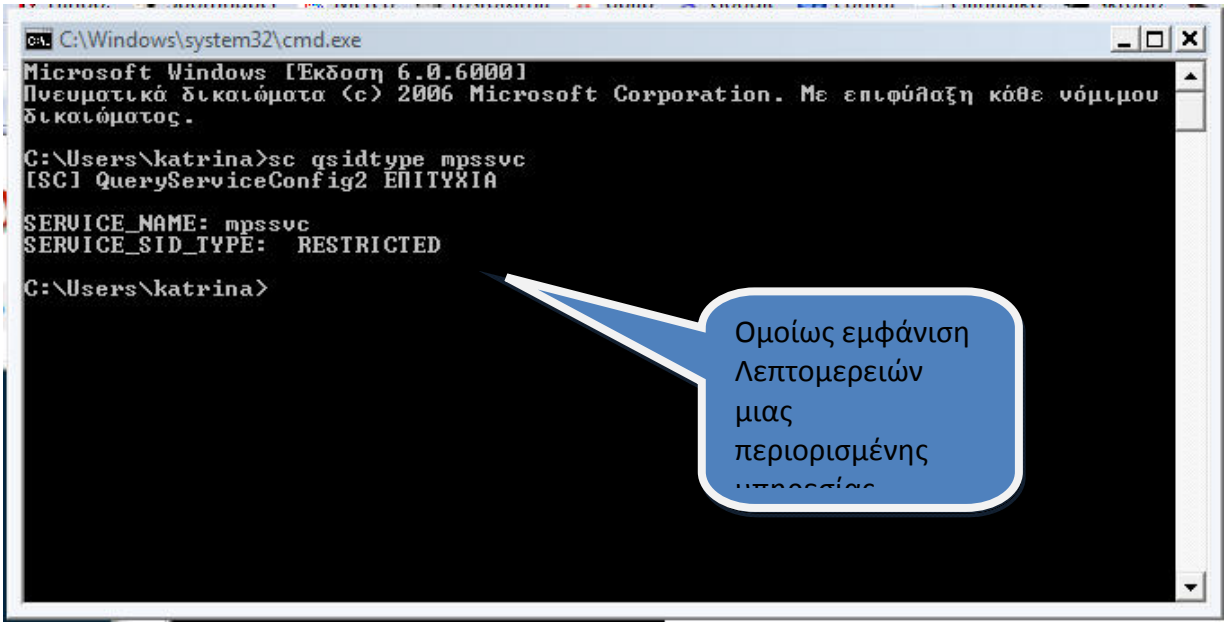
- Αρχικά πληκτρολογούμε την εντολή: **sc sidtype< service name > <restricted|unrestricted >**

- Εάν εν τω μεταξύ επιθυμούμε να δούμε τις ήδη υπάρχουσες ρυθμίσεις της υπηρεσίας αυτής πληκτρολογούμε την εντολή :**sc qsidtype<service name>** .

Παρακάτω παρουσιάζουμε δύο παραδείγματα τις εντολής αυτής ένα για την εμφάνιση πληροφοριών περιορισμένη υπηρεσία και ένα για μη περιορισμένη.

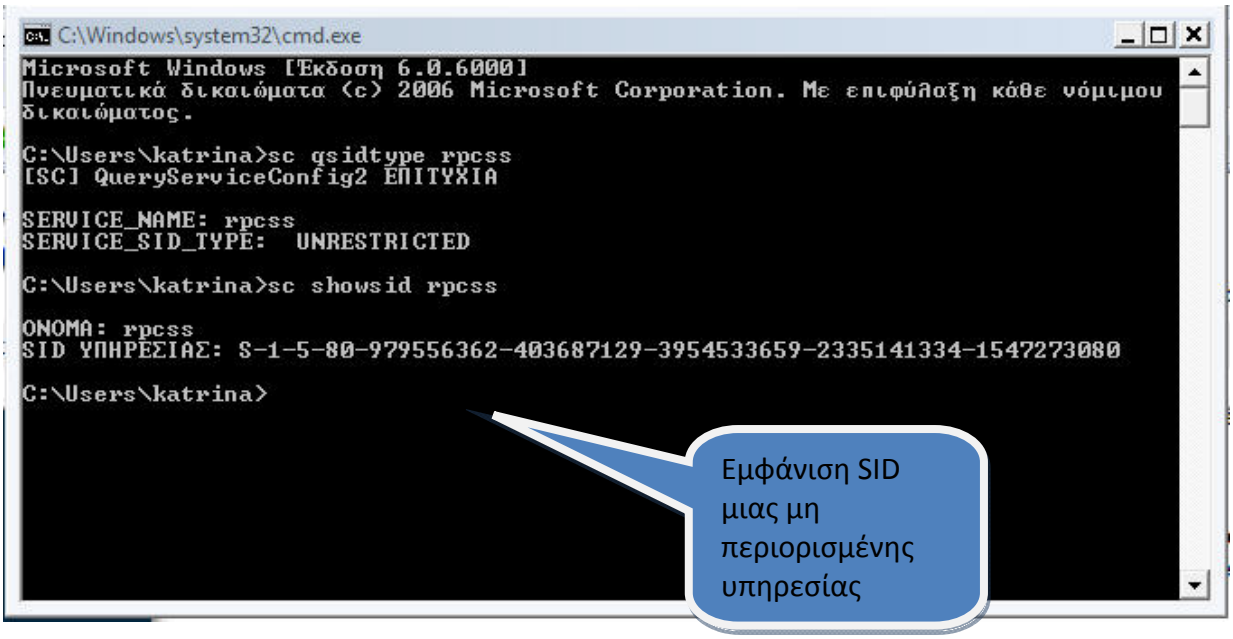


Εικόνα 89 : Παράθυρο 1ο εμφάνιση λεπτομερειών μην περιορισμένης υπηρεσίας.

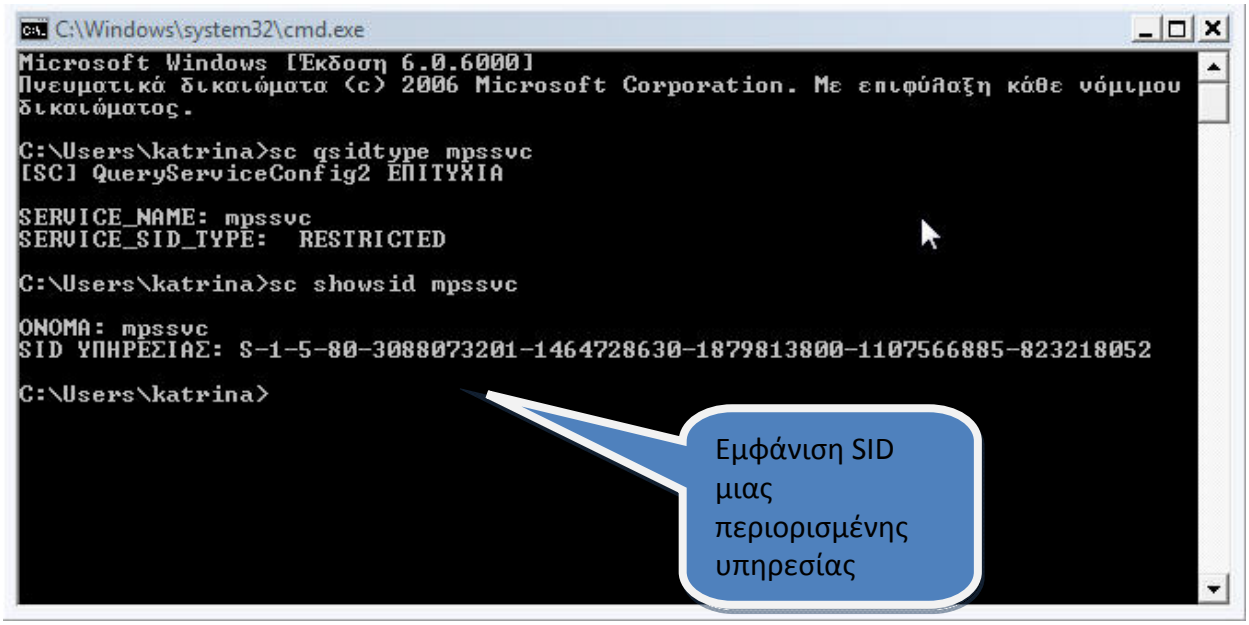


Εικόνα 90: Παράθυρο 2ο εμφάνιση λεπτομερειών περιορισμένης υπηρεσίας.

Στην συνέχεια εάν οι υπηρεσία είναι ρυθμισμένη να έχει προσωπική SID (ασχέτως με το αν η υπηρεσία είναι περιορισμένη ή όχι) τότε η υπηρεσία είναι προγραμματισμένη έτσι ώστε να χρησιμοποιεί SHA-1 hash.
Για να δούμε την SID μιας υπηρεσίας , χρησιμοποιούμε την **sc showsid <service name>** εντολή η οποία μας εμφανίζει τα ακόλουθα αποτελέσματα.



Εικόνα 91 : Παράθυρο εμφάνισης προσωπικής SID μιας περιορισμένης υπηρεσίας.



Εικόνα 92: Παράθυρο εμφάνισης προσωπικής SID μιας περιορισμένης υπηρεσίας.

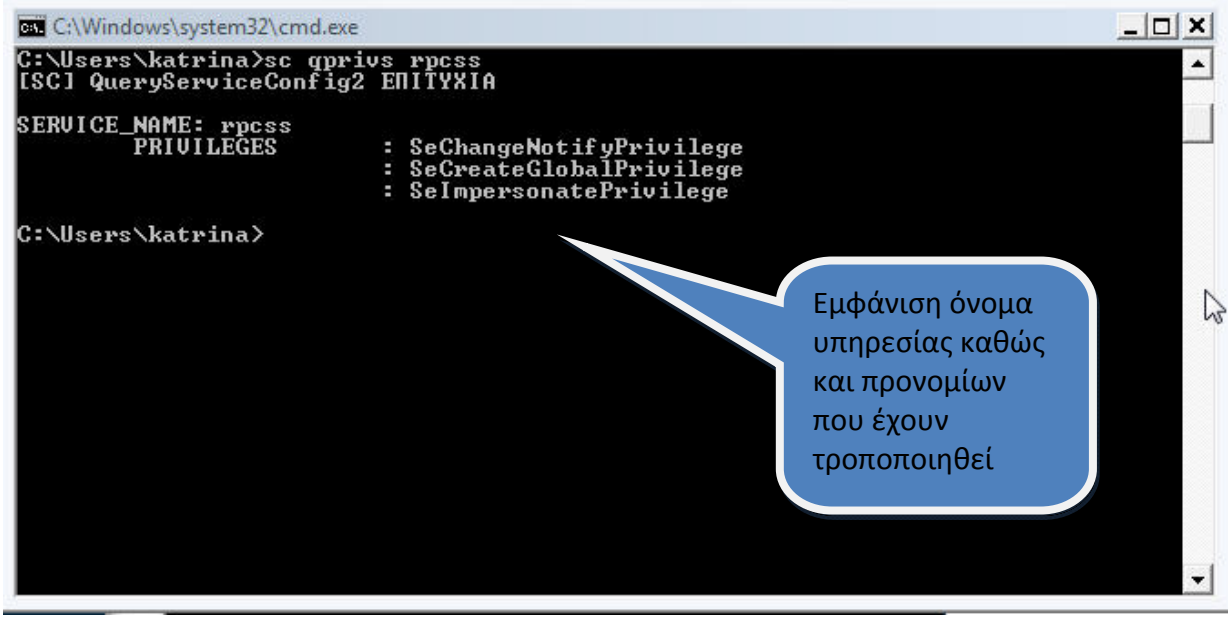
Στην υπηρεσία η οποία έχει ρυθμιστεί να διαθέτει προσωπική SID μπορεί να χορηγηθεί πρόσβαση σε πόρους τους οποίους χρειάζεται η υπηρεσία αυτή .
Στην προγενέστερη των Windows Vista εποχή , εάν μια υπηρεσία έτρεχε σε λογαριασμούς όπως πχ ο Local Service ή ο Network Service , ήταν αναγκαίο να τους δοθεί άδεια πρόσβασης για τους πόρους αυτούς , αυτό σημαίνει ότι όλες οι υπηρεσίες οι οποίες έτρεχα στο πλαίσιο αυτών των λογαριασμών διέθεταν επίσης άδεια πρόσβασης . Με αποτέλεσμα πολλές υπηρεσίες να διαθέτουν άδεια σε πολλά και μη αναγκαία σημεία του συστήματος μας.

Για να διορθωθεί το πρόβλημα αυτό , οι διαχειριστές ξεκινούσαν να διαχειρίζονται συγκεκριμένους λογαριασμούς οι οποίοι ήταν αφιερωμένοι σε συγκεκριμένες υπηρεσίες και οι οποίοι διέθεταν ιδιαίτερα διοικητικά προνόμια .
Με τον μηχανισμό προσωπικών SID , οι λογαριασμοί αυτοί μπορούν να χρησιμοποιηθούν, διαθέτοντας επιπλέον προνόμια , μέσω των προσωπικών SID και είναι ικανοί να ρυθμίσουν και να αποθηκεύσουν τις πληροφορίες αυτές , στις ACL`s το πόρων αυτών για την συγκεκριμένη υπηρεσία.

Όταν θέλουμε να χρησιμοποιήσουμε συντάκτη της ACL για τα αρχεία συστήματος ή για την registry , μπορούμε να πληκτρολογήσουμε την ακόλουθη εντολή για να προσδιορίσουμε την SID της υπηρεσίας και να την προσθέσουμε στον πόρο που επιθυμούμε : **NT SERVICE\<service name>.**

7.3.6.2 Αφαίρεση μη αναγκαίων προνομίων ανά υπηρεσία.

Στα Windows Vista και στον Windows Server 2008 , μια νέα τιμή της registry παρέχεται για να προσδιορίσει τα ακριβή προνόμια τα οποία η υπηρεσία θα πρέπει να διαθέτει και να λειτουργεί με αυτά . Η νέα αυτή τιμή ονομάζεται **RequiredPrivileges .** Η διαδικασία hosting της υπηρεσίας γνωρίζει μόνο τα προνόμια αυτά τα οποία προσδιορίζει η τιμή της registry .
Σε αυτό το σημείο πρέπει να σημειωθεί ότι ο μηχανισμός των **RequiredPrivileges** μπορεί να χρησιμοποιηθεί μόνο για να αφαιρέσει και ως αποτέλεσμα να μειώσει τα προνόμια μιας υπηρεσίας και όχι για να τα αυξήσει.
Εάν λοιπόν η τιμή **RequiredPrivileges** αναφερθεί σε προνόμια τα οποία δεν τα έχει ήδη η υπηρεσία , τότε τα προνόμια αυτά αγνοούνται . Η τιμή αυτή (**RequiredPrivileges**) αποθηκεύεται σε ένα ξεχωριστό για κάθε υπηρεσία ρυθμιστικό κλειδί το οποίο βρίσκεται : HKLM\System\CurrentControlSet\Services.
Ο **ChangeServiceConfig2 API** ή η εντολή **sc** μπορούν και σε αυτήν την περίπτωση να χρησιμοποιηθούν σε περίπτωση που επιθυμούμε να τροποποιήσουμε και να δούμε τα προνόμια αυτά.
Για να διαμορφώσουμε τα προνόμια αυτά για μία υπηρεσία πληκτρολογούμε την εντολή : **sc privs<service name><privileges>** όπως παρακάτω :



Εικόνα 93 : Παράθυρο τροποποίησης προνομίων μιας υπηρεσίας.

Ο καθορισμός των ποιων προνομίων είναι απαραίτητα για μια υπηρεσία και ποιων όχι είναι μια δύσκολη δουλειά , σε πολλές περιπτώσεις μπορεί να το επιλέξουμε κάποια προνόμια δοκιμαστικά και σε κάποιες άλλες περιπτώσεις μπορεί ακόμη και οι επιλογές να είναι λάθος.
Η τεκμηρίωση SDK των Windows μελετά σε πολλές περιπτώσεις τα προνόμια τα οποία είναι απαραίτητα όταν εργαζόμαστε με μια συγκεκριμένη API , παρόλο που τα προνόμια αυτά θα πρέπει να είναι ενεργά πριν από την κλήση της API . Αυτό λοιπόν που μας ζητείται είναι να μην ξεκινάμε να κάνουμε αλλαγές στα προνόμια των εφαρμογών χωρίς να τα έχουμε δοκιμάσει σε ένα απομονωμένο περιβάλλον.
Τέλος υπάρχουν ακόμη κάποιες καταστάσεις οι οποίες εμφανίζονται στην ευρεία περιοχή ενός λογαριασμού χρήστη και οι οποίες απασχολούν τους χρηστές .
Όπως παραδείγματος χάριν πότε μια υπηρεσία μπορεί να θεωρηθεί έμπιστη, ή ποτέ χρειάζεται πρόσβαση σε έναν απομακρυσμένο πόρο όπως επιτρέποντας στην Performance Logs and Alerts service να θέσει μια ερώτηση σε μια απομακρυσμένη μηχανή κ.α.

7.3.6.3 Παροχή γραπτού περιορισμένου σημείου πρόσβασης σε μια διαδικασία υπηρεσίας

Το τελευταίο κομμάτι με το οποίο θα ασχοληθούμε έχει να κάνει με την παροχή γραπτού περιορισμένου σημείου πρόσβασης σε μια διαδικασία υπηρεσίας .
Αυτό το σημείο πρόσβασης μπορεί να χρησιμοποιηθεί όταν οι ρυθμίσει του αντικειμένου που γραφτούν από την υπηρεσία είναι οριακές και μπορούν να διαμορφωθούν .

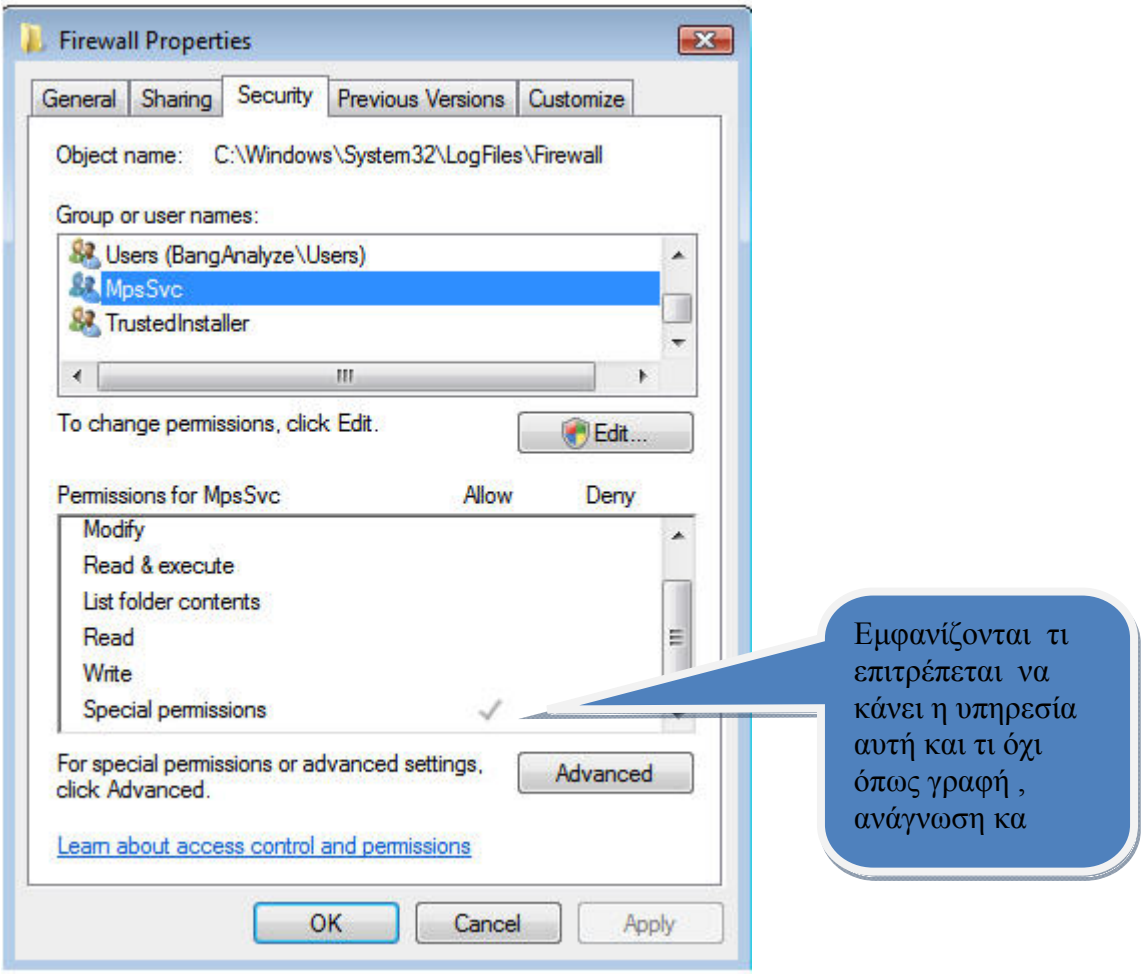
Μια προσπάθεια να γράψουμε σε έναν πόρο ο οποίος έχει ρητά επιχορηγηθεί με μια υπηρεσία SID πρόσβασης , θα αποτύχει . Ένα σημαντικό σημείο που πρέπει να αναφέρουμε εδώ είναι ότι ένα γραπτώς περιορισμένο σημείο είναι περιορισμένο μόνο από το να έχουν πρόσβαση και αν

μπορούν να γράψουν κάποιοι τύποι διαδικασιών . Είναι συνεπώς λιγότερο περιοριστικό από ένα περιορισμένο σημείο το οποίο περιορίζει όλων των τύπων των εισόδων .
Ένα γραπτώς περιορισμένο σημείο για μια ¨περιορισμένη¨ υπηρεσία θα έχει έναν από τους ακόλουθους τύπου SID περιορισμού : ανά-υπηρεσία SID , η logon SID, SID όλων και η νέα γραπτός περιορισμένη SID **(S-1-5-33 ή NT AUTHORITY\WRITE RESTRICTED)**
Η ανά-υπηρεσία SID και γραπτώς περιορισμένη SID είναι επίσης προσθεμένες στο Group SID`s .

Η γραπτώς περιορισμένη SID παρέχει τις ακόλουθες λειτουργίες :

- Η γραφή παρέχεται μόνο σε μερικούς τύπους της υπηρεσίας όπως στη logon SID, SID όλων ακόμη και στη νέα γραπτώς περιορισμένη SID . Δεν παρέχεται στον λογαριασμό υπηρεσίας ούτε στα γκρουπ.
- Η γραπτώς περιορισμένη SID επιτρέπει την χορήγηση πρόσβασης σε γραπτώς περιορισμένες υπηρεσίες.
- Εξ ορισμού , η γραπτώς περιορισμένη υπηρεσία δεν παρέχει σε μερικές υπηρεσίες SID την πρόσβαση σε πολλούς πόρους την οποίαν κανονικά θα έπρεπε να διέθεταν .Θα πρέπει να έτσι να επαναχορηγούμε γραπτή πρόσβαση στις υπηρεσίες αυτές , στα logon SIDs , στις γραπτώς περιορισμένες class ή στα Everyone group με σκοπό να έχουν δικαίωμα να γράψουν στους πόρους αυτούς .

Το μειονέκτημα του να χρησιμοποιούμε γραπτώς περιορισμένες SID`s είναι ο χρόνος που χρειάζονται για να εφαρμοστούν .
Θα πρέπει να καθορίσουμε όλες τις γραπτές προσβάσεις τις οποίες μια υπηρεσία χρειάζεται για να της παρέχονται οι προσβάσεις αυτές . Μέσα στα Windows Vista και τον Windows Server 2008 , υπάρχουν λίγες μόνο υπηρεσίες οι οποίες ορίζονται εξ ορισμού ως γραπτώς περιορισμένες .
Μια τέτοια υπηρεσία είναι η Windows Firewall υπηρεσία (της οποίας η συντομογραφία είναι MPSSVC).
Από τότε που η Windows Firewall υπηρεσία είναι γραπτώς περιορισμένη στους μόνους πόρους στους οποίους μπορεί να γράψει και στους οποίους μπορεί να έχει πρόσβαση είναι αυτοί που βασίζονται σε κάποιους συγκεκριμένους κανόνες .
Μια τέτοια τοποθεσία είναι ο φάκελος ο οποίος φιλοξενεί τα log file για το Firewall (**c:\Windows\Ssystem32\LogFiles\Firewall**) . Εάν προσέξουμε την ταμπέλα ασφαλείας για αυτόν το φάκελο θα παρατηρήσουμε ότι ο MPSSVC λογαριασμός έχει ρητά χορηγηθεί με δικαιώματα τα οποία φαίνονται στο παρακάτω παράθυρο :



Εικόνα 94 : Παράθυρο εμφάνισης αδειών πρόσβασης για το Windows Firewall.

7.3.7 Γιατί είναι σημαντική η υπηρεσία Windows Service Hardening

Σε αυτό το κομμάτι θα εξηγήσουμε , περιγράφοντας κάποιες γνωστές απειλές , γιατί το Service Hardening είναι μια πολύ χρήσιμη και αναγκαία υπηρεσία καθώς και πως μας κρατά ασφαλισμένους από συγκεκριμένες απειλές.

Οποιοσδήποτε ασχολείτο με την ασφάλεια των Windows IT (ή γενικά με οποιαδήποτε κομμάτι των Windows IT) θα έχει αναμφίβολα γνωριστεί με τις γνωστές απειλές **¨σκουλήκια (worms)¨** με το όνομα **Blaster** , **Slammer** και **Sasser** . Και τα τρία από αυτά είναι πολύ καταστροφικά , απλώνονται ταχύτητα και προκαλούν πολύ μεγάλες καταστροφές τόσο στις εταιρίες όσο και στους μεμονωμένους χρήστες.
Επίσης έχουν και ακόμη ένα κοινό γνώρισμα , όλα στοχεύουν τις υπηρεσίες των Windows .
Είναι γνωστό ότι στις υπηρεσίες των Windows είχαν τεθεί ήδη ζητήματα ασφάλειας προτού εμφανιστούν τα worms και αποτελέσουν απειλή . Έχει γίνει αναφορά ότι πριν περίπου 10 χρόνια , ένας χάκερ κατέδειξε με προειδοποιητικά μηνύματα το πώς θα μπορούσε να χρησιμοποιήσει τις υπηρεσίες των Windows προκειμένου να πετύχει πρόσβαση σε κάποιο σύστημα . Η επίθεση ήταν

σχετικά απλή και περιλάμβανε αντικατάσταση ενός υπάρχον εκτελούμενου αρχείου (μιας υπηρεσίας) με κάποιο άλλο αρχείο του ίδιου ονόματος .

Αυτό το πρόγραμμα ,ήταν ρυθμισμένο να τρέχει κάτω από τον ίδιο λογαριασμό με την πραγματική υπηρεσία , η οποία σε αυτήν την περίπτωση ήταν Local System, και μπορούσε επομένως να κάνει οτιδήποτε το οποίο το Local System είναι σε θέση να κάνει , πχ όπως να τροποποιήσει τις υπογραφές των antivirus .
Όπως εξηγήσαμε και προηγουμένως , ο λογαριασμός Local System είναι ο πιο ισχυρός λογαριασμός στο σύστημα μας . Μπορεί να έχει πρόσβαση σε υψηλής σημασίας κλειδιά στην Registry των Windows , απογυμνώνοντας τους χρήστες και παρουσιάζοντας τα πιστοποιητικά τους σε άλλα συστήματα .

Όλα αυτά ακούγονται τρομακτικά. Τρέχοντας οι υπηρεσίες σε λογαριασμούς με χαμηλά προνόμια, είναι μια μέθοδος που βοηθάει να ανακουφιστεί αυτό το ιδιαίτερο πρόβλημα που δημιουργεί αυτού του είδους τα ζητήματα. Για παράδειγμα εάν ένας λογαριασμός χρήστη δημιουργηθεί για να χρησιμοποιηθεί από κάποια υπηρεσία , ο διαχειριστής θα πρέπει να διατηρήσει ένα password για αυτήν την υπηρεσία . Τυπικά , αυτό το password θα πρέπει να τεθεί ως στόχος να μην λήξει να είναι δηλαδή ενεργό . Αυτό το γεγονός δίνει στον επιτιθέμενο όσο χρόνο χρειάζεται για να καταφέρει να βρει το password αυτό του λογαριασμού χρήστη .

Ακόμη , ένας λογαριασμός χρήστη θα πρέπει συχνά να χορηγηθεί με πρόσθετα προνόμια για να επιτραπεί σε αυτόν να λειτουργήσει σαν λογαριασμός υπηρεσίας .\
Οι υπηρεσίες είναι όλες οι πλέον τρωτές γιατί τυπικά ξεκινάνε όταν τα λειτουργικά συστήματα ξεκινούν , και εξακολουθούν να τρέχουν μέχρι να τεθούν εκτός λειτουργίας τα λειτουργικά συστήματα . Όχι μόνο για αυτόν τον λόγο , αλλά και γιατί πολλές υπηρεσίες τρέχουν σε αρκετά συστήματα , έτσι ώστε τα worms έχουν ένα μεγάλο αριθμό από διαθέσιμους υπολογιστές με σκοπό να προσβάλλουν . Με πολλούς τρόπους , οι υπηρεσίες αντιπροσωπεύουν τις τέλειες επιθέσεις επιφάνειας για τους χάκερ .

7.4 Επικύρωση - Authentication

Ο όρος Authentication (προέρχεται από την ελληνική λέξη ¨αυθεντικός¨) , και δηλώνει την πράξη μέσω της οποίας καθιερώνεται ή επιβεβαιώνεται (ως προς το περιεχόμενο του ή ως προς τον ιδιοκτήτη του) κάτι ή κάποιος . Επιβεβαιώνεται ότι είναι ¨αυθεντικός¨ δηλαδή ότι οι ισχυρισμοί που γίνονται προς ή από αυτόν είναι ορθοί και ισχύουν .
Η επικύρωση ενός αντικειμένου σημαίνει ότι επιβεβαιώνεται η προέλευσή του , εκτιμώντας ότι η επιβεβαίωση ενός προσώπου συχνά αποτελείται από την επαλήθευση της ταυτότητας του, ότι η προέλευση δηλαδή ενός χειροποίητου αντικειμένου είναι έμπιστη ή ακόμη η βεβαίωση ότι ένα πρόγραμμα υπολογιστών είναι αξιόπιστο.

Η διαδικασία της επικύρωσης εξαρτάται από έναν ή περισσότερους παράγοντες επικύρωσης .
Στα ιδιωτικά και δημόσια δίκτυα υπολογιστών, η επικύρωση γίνεται συνήθως μέσω της χρήσης της **¨σύνδεσης με κωδικό πρόσβασης ¨** . Η γνώση του κωδικού πρόσβασης υποτίθεται ότι εγγυάται ότι ο χρήστης είναι αυθεντικός . Η αδυναμία μέσω αυτού του τρόπου επικύρωσης , για τις συναλλαγές μας είναι ότι οι κωδικοί πρόσβασης μπορούν συχνά να κλαπούν ή να αποκαλυφθούν τυχαία . Για τον λόγο αυτό , στις χρήσεις μας στο διαδίκτυο καθώς και σε όλων

των ειδών τις συναλλαγές μας , απαιτείται μια αυστηρότερη διαδικασία επικύρωσης , η οποία θα μας εξασφαλίζει καλύτερη και ισχυρότερη ασφάλεια . Παράδειγμα πιο σύνθετων επικυρώσεων είναι η χρήση **Ψηφιακού Πιστοποιητικού** , το οποίο εκδίδεται και ελέγχεται από μια αρχή πιστοποιητικών .
Υπάρχουν πολλοί τομείς στους οποίους είναι απαραίτητη η επικύρωση όπως παραδείγματος χάριν στα προϊόντα , στις συναλλαγές χρημάτων στις χρήσεις των πιστωτικών καρτών και σε άλλα . Οι τομείς στου οποίους χρησιμοποιούμε την επιβεβαίωση και θα μας απασχολήσουν εμάς είναι η επιβεβαίωση που χρησιμοποιούμε για την ασφάλεια των υπολογιστών μας (computer security) , για την επιβεβαίωση του ελέγχου πρόσβασης(access control) στο σύστημα μας . Μελετώντας τόσο την απλή επικύρωση όσο και αυτές των δύο ή πολλαπλών παραγόντων (two-factor authentication) .
Στα ιδιωτικά και δημόσια δίκτυα ,τα οποία περιλαμβάνονται στο Διαδίκτυο, επικύρωση επιτυγχάνεται συνήθως με την χρήση κωδικών πρόσβασης για την σύνδεση. Η γνώση των κωδικών αυτών από κάποιον χρήστη δείχνει ότι ο χρήστης αυτός είναι αυθεντικός.

Η επικύρωση , όπως προαναφέραμε , είναι η διαδικασία με την οποία επαληθεύεται η ταυτότητα κάποιου ατόμου (μια διαδικασία η οποία δεν πρέπει να μπερδεύεται με την διαδικασία της έγκρισης , η οποία μας επαληθεύει τι μπορεί ένας χρήστης να κάνει, αν και οι όροι αυτοί έχουν χρησιμοποιηθεί εναλλακτικά).
Η επικύρωση απασχόλησε τους IT επαγγελματίες για δεκαετίες .Οι κωδικοί (passwords) είναι πάντα το βασικό κομμάτι στην διαδικασία της επικύρωσης σχεδόν σε όλα τα περιβάλλοντα εργασίας . Οι κωδικοί χρησιμοποιούνται για να διασφαλίζουν τα συστήματα μας ασφαλέστερα , σε πολλές περιπτώσεις είναι ο μόνος τρόπος ελέγχου και προστασίας των προσωπικών μας δεδομένων από την μη εξουσιοδοτημένη πρόσβαση τους . Όταν δακτυλογραφηθούν οι σωστοί κωδικοί στα πλαίσια των δικαιωμάτων εισόδων τότε χορηγείται πρόσβαση στο εν λόγω σύστημα σε αντίθετη περίπτωση η πρόσβαση είναι μη εξουσιοδοτημένη .
Με το πέρασμα των χρόνων έχει παρατηρηθεί ότι οι ανάγκες για ισχυρότερη ασφάλεια όλο και αυξάνονται . Οι προχωρημένοι χρήστες διαπιστώνουν ότι οι κωδικοί πρόσβασης είναι εύκολο να προσπελαστούν , και σε περιπτώσεις που οι χρήστες προσπαθήσουν να βάλουν έναν σύνθετο κωδικό για μεγαλύτερη ασφάλεια , αντιμετωπίζουν στην συνέχεια προβλήματα στον να τον θυμούνται .
Για τους λόγους αυτούς με το πέρασμα των χρόνων η προσπάθεια των χρηστών για ασφαλέστερα μηχανήματα τους οδηγεί σε πιο σύνθετες μεθόδους πιστοποίησης , όπως αυτήν των διπλών παραγόντων κα.

7.4.1 Επικύρωση ενός αντικειμένου .

Σε διάφορες πτυχές της καθημερινότητας όπως στην συναλλαγές μας με διάφορες υπηρεσίες , στην τέχνη , στην ανθρωπολογία κα ένα κοινό πρόβλημα που ίσως να μας απασχολεί είναι ο έλεγχος της ταυτότητας του δημιουργού ή του ιδιοκτήτη ενός αντικειμένου . Ο έλεγχος δηλαδή ότι ένα δεδομένο χειροποίητο αντικείμενο παρήχθη από ένα ορισμένο πρόσωπο ή από μια ορισμένη ομάδα , ή σε μια ορισμένη θέση ή χρονική περίοδο της ιστορίας .
Για τους λόγους αυτούς εμφανίζονται κάποιες τεχνικές οι οποίες είναι σε θέσει να αποσαφηνίσουν αυτά τα ερωτήματα και να πιστοποιήσουν την αυθεντικότητα των χρηστών των εκάστοτε αντικειμένων .
Γενικά υπάρχουν δύο τύποι τέτοιων τεχνικών .
Ο πρώτος συγκρίνει τις ιδιότητες του εμφανιζόμενου αντικειμένου με αυτές του αντικειμένου που είναι γνωστό ως αυθεντικό . Για παράδειγμα , σε ένα έργο τέχνης για να πιστοποιηθεί η αυθεντικότητα του και να επικυρωθεί ο δημιουργός του , αναζητούνται και συγκρίνονται

ομοιότητες στο ύφος της ζωγραφικής , γίνεται έλεγχος της θέσης και της μορφής μιας υπογραφής του δημιουργού ή ακόμη συγκρίνεται το αντικείμενο αυτό με μια παλιά φωτογραφία του αυθεντικού αντικειμένου κα . Με τον τρόπο αυτό ελέγχετε η γνησιότητα του .
Ο δεύτερος τύπος τεχνικής στηρίζεται στην τεκμηρίωση άλλων εξωτερικών επιβεβαιώσεων , για παράδειγμα στο παράδειγμα που προαναφέραμε τα έργα τέχνης συνοδεύονται από κάποια πιστοποιητικά αυθεντικότητας τους . Τα αρχεία αυτά από την μια είναι ένας τρόπος πιστοποίησης της αυθεντικότητας των αντικειμένων αυτών , αλλά από την άλλη διαθέτουν και αυτά τρωτά σημεία , τα οποία μπορεί και να εκμεταλλευτούν από κακόβουλους χρήστες και να δεχτούν οποιαδήποτε είδους παραποίηση .
Ανάλογα με την περίσταση ή με τον τύπο των αντικειμένων γίνεται και η επιλογή του τύπου τεχνικής επικύρωσης που θα χρησιμοποιηθεί αναλυτικά οι τύποι θα παρουσιαστούν παρακάτω .

7.4.2 Επικύρωση για την ασφάλεια του υπολογιστή

Στον τομέα της ασφάλειας των υπολογιστών , η επικύρωση είναι μια διαδικασία που έχει ως στόχο να ελέγξει την **ψηφιακή ταυτότητα (digital identity)** του αποστολέα μιας επικοινωνίας όπως πχ το αίτημα να συνδεθεί . Ο αποστολέας που επικυρώνεται συχνά αναφέρεται και ως **προϊστάμενος** , αυτός εν τέλη που επικυρώνεται μπορεί να είναι είτε κάποιο πρόσωπο που χρησιμοποιεί ένα υπολογιστή, ή ο υπολογιστής ο ίδιος είτε ακόμη ένα πρόγραμμα που εκτελείται σε κάποιο υπολογιστή.
Από την άλλη πάλι, υπάρχει και το **Τυφλό Πιστοποιητικό (blind credential)** , σε αντίθεση όμως αυτό , δεν καθιερώνει καθόλου την ταυτότητα , αλλά μόνο ένα μικρό δικαίωμα ή την κατάσταση του χρήστη ή κάποιο πρόγραμμα.
Σε έναν Ιστοχώρο όπου υπάρχει εμπιστοσύνη , ¨η επικύρωση ¨ είναι ένας τρόπος για να διασφαλιστεί ότι οι χρήστες είναι αυτοί που στην πραγματικότητα λένε , επίσης διασφαλίζει ότι ο χρήστης ο οποίος επιχειρεί να εκτελέσει μια λειτουργία στο σύστημα είναι στην πραγματικότητα ο χρήστης που εξουσιοδοτείται για να εκτελέσει την λειτουργία αυτή.

7.4.3 Επικύρωση ελέγχου πρόσβασης

Μια άλλη γνωστή χρήση της επικύρωσης είναι για τον έλεγχο πρόσβασης . Ένα σύστημα υπολογιστή υποτίθεται ότι θα χρησιμοποιείται μόνο από αυτούς οι οποίοι είναι εγκεκριμένοι καθώς επίσης θα πρέπει να γίνονται προσπάθειες για να ανιχνεύονται και να αποκλείονται οι μη εγκεκριμένοι .Εντούτοις η πρόσβαση σε αυτό συνήθως κοντρολάρεται από επίμονες διαδικασίες επικύρωσης που καθιερώνουν με κάποιου καθιερωμένου βαθμού εμπιστοσύνης την ταυτότητα του χρήστη, και από εκεί χορηγούνται εκείνα τα προνόμια όπου θα μπορούσαν να εγκριθούν για εκείνη την ταυτότητα .
Κοινά παραδείγματα του ελέγχου πρόσβασης που περιλαμβάνουν την επικύρωση περιλαμβάνουν:

- Ανάληψη μετρητών από το ATM.
- Έλεγχος απομακρυσμένου υπολογιστή μέσω Διαδικτύου.

- Χρησιμοποίηση ενός Δια- τραπεζικού συστήματος Διαδικτύου.

Εντούτοις , πρέπει να σημειώσουμε ότι ένας μεγάλος μέρος της συζήτησης σχετικά με αυτά τα θέματα θα μπορούσε να χαρακτηριστεί παραπλανητική για τον λόγο ότι οι όροι χρησιμοποιούνται χωρίς μεγάλη ακρίβεια . Μέρος αυτής της σύγχυσης μπορεί να οφείλεται στον τόνο ¨επιβολή νόμου ¨ ενός μεγάλου μέρους της συζήτησης . Κανένας υπολογιστής , πρόγραμμα υπολογιστή ή χρήστης υπολογιστή , δεν μπορεί να επιβεβαίωση την ταυτότητα κάποιου άλλου ,τρίτου κατασκευαστή . Δεν είναι ακόμη δυνατόν να ¨καθιερώσει ¨ ή να ¨ αποδείξει ¨ μια ταυτότητα .Υπάρχουν δυσνόητα ζητήματα κρυμμένα κάτω από αυτά που εμφανίζονται να είναι μια απλή επιφάνεια .

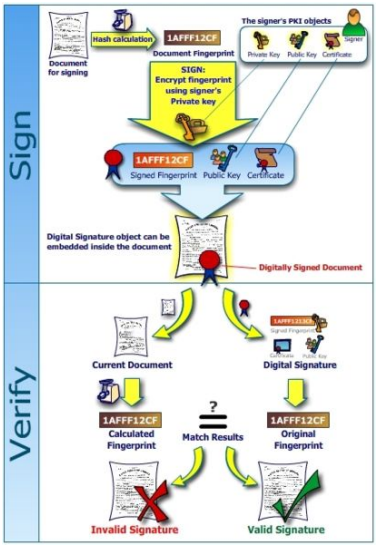
Είναι μόνο δυνατόν να εφαρμοστούν μια ή περισσότερες δοκιμές οι οποίες , εάν περαστούν , θα έχουν από την αρχή δηλωθεί ως επαρκής για να προχωρήσει . Το πρόβλημα είναι να δηλωθούν ποίες δοκιμές είναι επαρκείς και ποίες δεν είναι .΄Εχουν υπάρξει πολλές περιπτώσεις τέτοιων δοκιμών που έχουν αποτύχει και από την αποτυχία τους έχουν παρουσιαστεί , αναπόφευκτα, ότι είναι ανεπαρκής . Πολλοί άνθρωποι συνεχίζουν να θεωρούν τις δοκιμές αυτές επιτυχημένες και ρίχνουν το φταίξιμο της αποτυχίας στο ¨sloppiness¨ ή στην ανικανότητα σε κάποιο κομμάτι κάποιου.
Το πρόβλημα είναι ότι οι δοκιμές υποτίθεται ότι θα δούλευαν και στην πράξη , και όχι μόνο κάτω από ιδανικές συνθήκες ή χωρίς ¨sloppiness¨ ή λόγο ανικανότητας να μην δουλεύουν .Είναι οι δοκιμασίες που δεν δουλεύουν κάτω από αυτές τις συνθήκες και δεν οφείλεται στις προαναφερθείσες δικαιολογίες
Εξετάζοντας την πολύ κοινή περίπτωση ενός ηλεκτρονικού ταχυδρομείου επιβεβαίωσης το οποίο πρέπει να απαντηθεί προκειμένου να ενεργοποιηθεί ένας σε σύνδεση υπολογιστής κάποιου είδους . Δεδομένου ότι το ηλεκτρονικό ταχυδρομείο μπορεί εύκολα να κανονιστεί για να πάει ή να προέλθει από τις ψευδείς και μη εντοπίσημες διευθύνσεις αυτή είναι μια εξαιρετικά αδύνατη μέθοδος επικύρωσης .

7.4.4 Ορισμοί συσχετιζόμενοι με την Επικύρωση

7.4.4.1 Ψηφιακή Ταυτότητα (Digital Identity).

Καλό θα ήταν στο σημείο αυτό και προτού προχωρήσουμε στην ανάλυση του μηχανισμού επικύρωσης , να εξηγήσουμε κάποιους ορισμούς που συναντήσαμε ή πρόκειται να συναντήσουμε στην συνέχεια.
Αρχικά θα ασχοληθούμε με τον όρο Ψηφιακή ταυτότητα . Ο όρος αυτός αναφέρεται στην πτυχή της ψηφιακής τεχνολογίας η οποία ασχολείται με την μεσολάβηση της εμπειρίας των ανθρώπων , της δικής τους ταυτότητας καθώς και την ταυτότητα άλλων ανθρώπων και πραγμάτων . Η ψηφιακή ταυτότητα έχει επίσης μια ακόμη γνωστή χρήση ,ως την ψηφιακή αντιπροσώπευση ενός συνόλου από ισχυρισμούς οι οποίοι έχουν δημιουργηθεί από ένα ψηφιακό αντικείμενο και αφορούν είτε αυτό το ίδιο το αντικείμενο ή κάποιο άλλο ψηφιακό αντικείμενο .

7.4.4.2 Ψηφιακή Υπογραφή (Digital Signature).



Εικόνα 95 : Ψηφιακή υπογραφή .

Ψηφιακή υπογραφή ή αλλιώς ψηφιακό σχέδιο υπογραφών , είναι ένας τύπος ασύμμετρου συστήματος κρυπτογραφίας που χρησιμοποιείται για να μιμηθεί τις ιδιότητες ασφάλειας μιας χειρόγραφης υπογραφής σε κάποιο έγγραφο. Τα ψηφιακά σχέδια υπογραφών αποτελούνται από τουλάχιστον τρείς αλγόριθμους : Έναν βασικό αλγόριθμο παραγωγής , ένα αλγόριθμο υπογραφών και ένα αλγόριθμο επαλήθευσης .Μια υπογραφή παρέχει επικύρωση σε ένα μήνυμα. Το μήνυμα αυτό μπορεί να είναι οτιδήποτε από ένα ηλεκτρονικό e-mail ή μια σύμβαση ή ακόμη και ένα μήνυμα που στέλνετε σε ένα πιο περίπλοκο κρυπτογραφικό πρωτόκολλο.
Οι ψηφιακές υπογραφές χρησιμοποιούνται συχνά για να εφαρμόσουν τις ηλεκτρονικές υπογραφές , ένας ευρύτερος όρος ό οποίος αναφέρεται σε οποιοδήποτε ηλεκτρονικό δεδομένο φέρνει την πρόθεση μιας υπογραφής , αλλά δεν ισχύει πάντα ότι όλες οι ηλεκτρονικές υπογραφές χρησιμοποιούν ψηφιακές υπογραφές.
Σε μερικές χώρες συμπεριλαμβανομένης και της Ευρωπαϊκής Ένωσης , οι ηλεκτρονικές υπογραφές έχουν νομική σημασία . Εντούτοις οι νόμοι σχετικά με τις ηλεκτρονικές υπογραφές δεν καθιστούν πάντα δυνατή την εφαρμογή τους σε σχέση με τις κρυπτογραφικές υπογραφές , πράγμα που τις αφήνει νομικά κάπως απροσδιόριστες.

7.4.4.3 Ψηφιακό Αντικείμενο (Digital Subject).

Με τον όρο ψηφιακό αντικείμενο εννοούμε μια οντότητα αντιπροσωπευόμενη ή υπαρκτή στην ψηφιακή σφαίρα και η οποία παρουσιάζεται να περιγράφεται ή να εξετάζεται . Κάθε ψηφιακό αντικείμενο έχει έναν πεπερασμένο αριθμό από ιδιότητες ταυτότητας . Το ψηφιακό αντικείμενο μπορεί να είναι κάτι ανθρώπινο ή μη ανθρώπινο . Παραδείγματα μη ανθρώπινων ψηφιακών αντικειμένων είναι:

- Συσκευές και υπολογιστές.

- Ψηφιακοί πόροι.
- Πολικές και σχέσεις μεταξύ άλλων ψηφιακών αντικειμένων .

7.4.4.4 Επικύρωση, Έγκριση, Έλεγχος πρόσβασης.

Τρία κριτήρια άμεσα συνδεδεμένα μεταξύ τους ,και τα τρία χρησιμοποιούνται έμμεσα ή άμεσα με την πιστοποίηση και επικύρωση των δεδομένων . Κύριο μέλημα τους είναι να εξασφαλίζουν τόσο την αυθεντικότητα των ιδιοκτητών των δεδομένων όσο και να οδηγούν τα δεδομένα ή τα αιτήματα στους πόρους στους οποίους πραγματικά προορίζονται .

Τα κριτήρια αυτά καλούνται Έγκριση , Επικύρωση, Έλεγχος πρόσβασης .
Επικύρωση είναι οποιαδήποτε διαδικασία τίθεται σε λειτουργία προκειμένου να ελέγχετε ότι κάποιος ή κάτι είναι αυτό που πραγματικά ισχυρίζεται . Αυτή η διαδικασία συνήθως απαιτεί , ένα όνομα χρήστη και έναν κωδικό πρόσβασης , αλλά μπορεί να περιλαμβάνει και οποιοδήποτε άλλη μέθοδο ταυτοποίησης όπως μια έξυπνη κάρτα , ανίχνευση αμφιβληστροειδή , αναγνώριση φωνής ή ακόμη και τα δακτυλικά αποτυπώματα .
Η έγκριση , εγκρίνει εάν το πρόσωπο , αφού αυτό αρχικά έχει επικυρωθεί , εάν του επιτρέπεται να έχει στην κατοχή του κάποιον πόρο . Αυτό καθορίζεται συνήθως με τον προσδιορισμό της ομάδας της οποίας είναι μέλος το πρόσωπο αυτό . Εάν το πρόσωπο – χρήστης πληρεί τα ασφαλή επίπεδα λειτουργίας και δεν είναι επιβλαβές για το σύστημά μας , τότε είναι αποδεχτό και του επιχορηγείται η έγκριση. Η διαδικασία της έγκρισης είναι μια διαδικασία αντίστοιχη του ελέγχου του εισιτηρίου μας στην είσοδο ενός θεάτρου .
Τέλος η διαδικασία του ελέγχου πρόσβασης , είναι ένας γενικότερος τρόπος ελέγχου πρόσβασης μας σε ένα πόρο του Ιστού . Η πρόσβασή μας σε αυτόν τον πόρο , μπορεί είτε να χορηγηθεί ,είτε να απαγορευτεί η απόφαση αυτή είναι βασισμένη σε μια σειρά από κριτήρια, όπως η διεύθυνση δικτύου του πελάτη, η χρονική στιγμή προσπέλασης αυτού , η μηχανή αναζήτησης που αυτός χρησιμοποιεί κ.α. . Ο έλεγχος πρόσβασης είναι συσχετισμένος με διαδικασίες όπως το κλείσιμο της πύλης κάποιου προορισμού με την λήξη του χρόνου προθεσμίας υποβολής , γενικά ελέγχεται η είσοδος ή όχι με βάση κάποιους αυθαίρετους όρους που μπορεί να πληρεί ή όχι ο εκάστοτε επισκέπτης .
Επειδή αυτές οι τρείς τεχνικές είναι τόσο στενά συνδεδεμένες ,στις περισσότερες πραγματικές εφαρμογές είναι πολύ δύσκολο να ξεχωρίσουμε την μια από την άλλη . Στην πραγματικότητα , η επικύρωση και η έγκριση είναι , στις περισσότερες εφαρμογές, είναι ταυτόσημες .

7.4.4.5 Επικύρωση (Authentication) Vs Έγκριση (Authorization).

Με την πρώτη ματιά είναι σχετικά δύσκολο να ξεχωρίσουμε ακριβώς τους δύο αυτούς ορισμούς , της επικύρωσης και της έγκρισης .Παρόλα αυτά στο σημείο αυτό θα κάνουμε μια προσπάθεια να αποσαφηνίσουμε τα πράγματα .
Για να διακρίνουμε τον όρο επικύρωση από τον στενά συσχετιζόμενο όρο ¨έγκριση¨, οι συντομογραφίες A1 (Επιβεβαίωση) και A2(Εγκριση) ,χρησιμοποιούνται περιστασιακά . Επίσης οι όροι AuthN / AuthZ ή Au /Az χρησιμοποιούνται σε μερικές κοινότητες προκειμένου να επιτευχθεί ο διαχωρισμός αυτός.

Το πρόβλημα της έγκρισης, είναι συχνά το ίδιο με αυτό της επικύρωσης, πολλά ευρέως υιοθετημένα πρωτόκολλα ασφάλειας , υποχρεωτικοί κανονισμοί και ακόμη και τα καταστατικά είναι βασισμένα σε αυτήν την υπόθεση . Εντούτοις , η πιο ακριβής χρήση περιγράφει την επικύρωση ως την διαδικασία επαλήθευσης της ταυτότητας του ατόμου , ενώ η έγκριση είναι μια διαδικασία η οποία επαληθεύει ότι ένα γνωστό άτομο έχει την δικαιοδοσία να εκτελέσει μια συγκεκριμένη λειτουργία. Η επικύρωση ,επομένως , πρέπει να προηγηθεί της έγκρισης .
Για παράδειγμα , μόνο όταν παρουσιάζουμε τα κατάλληλα προσδιοριστικά σε έναν αφηγητή μιας τράπεζας , μπορούμε να επικυρωθούμε από τον αφηγητή και να πάρουμε έγκριση προκειμένου να έχουμε πρόσβαση στις πληροφορίες του λογαριασμού τραπέζης μας . Δεν να μας δοθεί έγκριση πρόσβασης στον λογαριασμό εάν εκ τον προτέρων δεν έχουμε επικυρωθεί ότι είμαστε όντως εμείς οι κάτοχοι αυτού .
Μέχρι η έγκριση να μην μπορεί να λαμβάνει χώρα χωρίς την επικύρωση , ο πρώτος αναφερθείς όρος , δηλαδή η έγκριση , χρησιμοποιείται για να σημάνει τον συνδυασμό της επικύρωσης και της έγκρισης.

7.4.5 Επικύρωση Διπλών παραγόντων (Two-factor authentication).

Στο πεδίο τώρα των υπολογιστών, η μέθοδος της κρυπτογραφίας όσο και άλλες μέθοδοι (βλέπε ψηφιακές υπογραφές και επικύρωση πρόσκλησης-απάντησης) έχουν αναπτυχθεί .
Δεν είναι γνωστό εάν αυτές οι μέθοδοι επικύρωσης οι οποίες είναι βασισμένες στην κρυπτογραφία είναι ευαπόδεικτα ασφαλής δεδομένου ότι οι απρόβλεπτες μαθηματικές εξελίξεις μπορούν να τις καταστήσουν τρωτές σε επιθέσεις στο μέλλον . Εάν αυτό αποδειχτεί , μπορεί να θέσει υπό αμφισβήτηση ένα μεγάλο μέρος της επικύρωσης του παρελθόντος.
Για παράδειγμα μια ειδική περίπτωση στην ψηφιακής επικύρωσης ,που γίνεται χρήση μια ψηφιακά υπογεγραμμένη σύμβαση , αυτού του είδους η επικύρωση μπορεί να υποστεί συμβιβασμό μόνο όταν ανακαλυφθεί μια νέα επίθεση στο σύστημα κρυπτογραφίας η οποία να κρύβεται κάτω από μια υπογραφή .

Ο **παράγοντας επικύρωσης** είναι ένα κομμάτι των πληροφοριών και της διαδικασίας που χρησιμοποιείται για να επικυρώσει ή να ελέγξει την ταυτότητα ενός προσώπου για λόγους ασφάλειας. . Ο διπλός παράγοντας επικύρωσης (T-FA) , είναι ένα σύστημα όπου δυο διαφορετικοί παράγοντες χρησιμοποιούνται για να επικυρώσουν . Η χρησιμοποίηση δύο παραγόντων σε αντιδιαστολή με το ένα παραδίδει έναν υψηλότερου επιπέδου μηχανισμό επικύρωσης . Η χρησιμοποίηση περισσότερων του ενός παραγόντων καλείται μερικές φορές και ¨ Ισχυρή επικύρωση¨.
Οι **ανθρώπινοι παράγοντες επικύρωση** είναι γενικά ταξινομημένοι σε τρείς περιπτώσεις :

- Κάτι που ο χρήστης έχει (πχ ID card, security token , software token, phone ή cell phone).
- Κάτι που ο χρήστης γνωρίζει(πχ password , pass phrase ή PIN –Personal identification number)
- Κάτι που ο χρήστης είναι ή κάνει (πχ fingerprint ή retinal pattern, DNA, signature ή voice recognition ή biometric identifier).

Συχνά χρησιμοποιείται ο συνδυασμός των μεθόδων αυτών .Ιστορικά τα αποτυπώματα (fingerprint) είναι η πιο επιτακτικά χρησιμοποιημένη μέθοδος επικύρωσης , αλλά οι πρόσφατες δικαστικές υποθέσεις τόσο στις ΗΠΑ όσο και αλλού, εκφράζουν θεμελιώδεις αμφιβολίες για την αξιοπιστία των δακτυλικών αποτυπωμάτων .Επίσης οι βιομετρικές μέθοδοι δείχνουν να είναι ελπιδοφόρες αλλά έχουν παρουσιαστεί στην πράξη να είναι εύκολα να παρακαμφθούν .

Άλλοι παράγοντες επικύρωσης περιλαμβάνουν:

- Κοινωνική δικτύωση.
- Ένας έμπιστος ιστός που διαμορφώνει τις σχέσεις μεταξύ των πιστοποιητικών επικύρωσης .
- Η επικύρωση βασισμένη στην θέση , όπως για παράδειγμα αυτή που υιοθετείται από τις επιχειρήσεις πιστωτικών καρτών για να διασφαλίσει ότι μια κάρτα δεν χρησιμοποιείται σε δύο θέσεις την ίδια χρονική στιγμή.
- Η επικύρωση βασισμένη στον χρόνο , η οποία επιτρέπει την πρόσβαση ή όχι κατά την διάρκεια κάποιων συγκεκριμένων ωρών .

Το να χρησιμοποιούμε ένα μόνο παράγοντα , για παράδειγμα ένα στατικό password , θεωρείται από μερικούς ως αδύναμη επικύρωση .Η ισχυρή επικύρωση περιλαμβάνει επίσης πολλαπλούς παράγοντες οι οποίοι δεν περιλαμβάνουν έναν φυσικό παράγοντα , όπως μία κάρτα . Οι πολλαπλοί παράγοντες μπορούν να είναι όλοι ταυτόχρονα σε λειτουργία για πιο ισχυρή επικύρωση .

Εντούτοις θα πρέπει να αναφερθεί , ότι η ισχυρή επικύρωση και η επικύρωση πολλαπλών παραγόντων είναι δύο πλήρως διαφορετικές διαδικασίες.
Οι υποστηριχτές της T-FA υποστηρίζουν ότι θα μπορούσαν να μειωθούν δραστικά οι επιπτώσεις της κλοπής της ταυτότητας ενώ βρισκόμαστε σε σύνδεση καθώς και σε άλλες απάτες που γίνονται online , και αυτό επειδή ο κωδικός πρόσβασης του θύματος δεν θα είναι πλέον σε θέση να δώσει στους κλέφτες πρόσβαση στις πληροφορίες .
Παρόλα αυτά ο T-FA είναι ακόμα τρωτός στα Trojan και στις κατά άτομο μέσες επιθέσεις.
Με το πέρασμα των χρόνων εμφανίστηκαν νέα εργαλεία επέκτασης του T-FA μηχανισμού όπως οι έξυπνες κάρτες και τα σημεία USB.
Οι περισσότεροι οργανισμοί προσθέτουν ένα στρώμα ασφάλειας στην επιφάνεια, το οποίο απαιτεί οι χρήστες να κατέχουν ένα σημείο της φυσικής διαδικασίας και να γνωρίζουν κάποιο PIN ή password με σκοπό να μπορούν ανά έχουν πρόσβαση στα δεδομένα.

Παρόλα αυτά υπάρχουν ακόμη μερικά μειονεκτήματα στον μηχανισμό επικύρωσης διπλών παραγόντων , τα οποία εμποδίζουν την εξάπλωση της τεχνολογίας αυτής .

7.4.5.1 Security Tokens – Σημεία Ασφάλειας.

Οι πιο κοινές μορφές των ανθρώπινων παραγόντων της κατηγορίας ¨κάτι που ο χρήστης έχει ¨, είναι οι έξυπνες κάρτες τα PIN και τα USB. Οι διαφορές αυτών μηχανισμών και τεχνολογιών είναι ελάχιστες . Αναλυτική περιγραφή όλων θα ακολουθήσει στην συνέχεια .

7.4.5.1.1 Πιστοποιητικά επικύρωσης

.

Πιστοποιητικά επικύρωσης.

Η χορήγηση πρόσβαση ενός χρήστη σε κάποιο σύστημα , όπως προαναφέραμε προαπαιτεί έλεγχο πρόσβασης επικύρωση , έγκριση κ.τ.λ. .Η ολοκλήρωση αυτών των μηχανισμών όμως απαιτεί την παροχή κάποιον απαραίτητων πιστοποιητικών . Η χορήγηση της πρόσβασης εξαρτάται άμεσα από αυτά τα πιστοποιητικά .

Τα πιστοποιητικά επικύρωσης είναι κάτι που γνωρίζουμε , όπως ο αριθμός PIN , κάτι που διαθέτουμε όπως ένα διακριτικό πρόσβασης , ή κάτι που διαθέτουμε σαν άτομα όπως ένα βιομετρικό χαρακτηριστικό ή ακόμη συνδυασμοί αυτών που προαναφέραμε .

Το χαρακτηριστικό πιστοποιητικό είναι μια κάρτα πρόσβασης, η οποιοδήποτε άλλο κλειδί .

Υπάρχουν πολλές τεχνολογίες καρτών συμπεριλαμβανομένης της μαγνητικής λωρίδας (magnetic stripe), των bar code, οι έξυπνες κάρτες επαφής και οι έξυπνες κάρτες μη επαφής . Ακόμη υπάρχουν οι τυπικές βιομετρικές τεχνολογίες , όπως τα δακτυλικά αποτυπώματα , η αναγνώριση προσώπων , η αναγνώριση ιρίδων ή του αμφιβληστροειδή , η ανίχνευση φωνής , η γεωμετρία χεριών κ.α. .

7.4.5.1.2 Τα PIN

Ο προσωπικός αριθμός αναγνώρισης (Personal Identification Number) εμπίπτει στην κατηγορία αυτού που ξέρουμε ότι διαθέτουμε .Το PIN είναι συνήθως ένας αριθμός που αποτελείται από τέσσερα έως οκτώ ψηφία. Όσο λιγότερα είναι τα ψηφία του κωδικού αυτού τόσο πιο εύκολο είναι να τα θυμάται ο χρήστης αλλά και το ίδιο εύκολα μπορούν να αποκτηθούν από κάποιο κακόβουλο χρήστη . Από την άλλη όσο περισσότερα ψηφία έχει τόσο δυσκολότερα υποκλέπτεται αλλά και δυσκολότερα απομνημονεύεται από τον χρήστη. Το πλεονέκτημα της χρησιμοποίησης του PIN ως πιστοποιητικό πρόσβασης είναι ότι μόλις απομνημονευτεί ο αριθμός το πιστοποιητικό αυτό δεν μπορεί ούτε να χαθεί ούτε να αφεθεί κάπου.

Το μειονέκτημα της τεχνολογίας αυτής είναι ότι οι χρήστες ίσως δυσκολεύονται να απομνημονεύουν αριθμούς που δεν χρησιμοποιούν συχνά . Τα PIN είναι ασφαλέστερη τεχνολογία από ότι αυτή των bar code ή των μαγνητικών λωρίδων .

7.4.5.1.3 Έξυπνες κάρτες και USB.

Έξυπνες κάρτες

Οι έξυπνες κάρτες είναι κάτι κάρτες σχεδόν στο ίδιο μέγεθος και σχήμα όπως μια πιστωτική κάρτα . Οι λειτουργία του ποικίλει ανάλογα με τις απαιτήσεις του κατασκευαστή .

Υπάρχουν δύο τύποι έξυπνων καρτών , αυτές της επαφής και αυτές της μη επαφής . Κατασκευαστικά και οι δύο τύποι διαθέτουν ένα ενσωματωμένο μικροεπεξεργαστή και μια μνήμη . Η έξυπνη κάρτα διαφέρει από την τυπικά αποκαλούμενη κάρτα εγγύτητας , δεδομένου ότι το μικροτσίπ στην κάρτα εγγύτητας έχει μια μόνο λειτουργία , να παρέχει στον αναγνώστη τον αριθμό αναγνώρισης της κάρτας . Ο επεξεργαστής σε μια έξυπνη κάρτα έχει ένα λειτουργικό σύστημα και χειριστεί πολλαπλάσιες εφαρμογές , όπως την λειτουργία μιας κάρτας μετρητών , μιας προπληρωμένης κάρτας , μιας κάρτας ιδιότητας μέλους ακόμη και μιας κάρτας ελέγχου πρόσβασης . Η διαφορά μεταξύ των δύο τύπων έξυπνων καρτών έγκειται στον τρόπο με τον οποίον ο μικροεπεξεργαστής στην κάρτα επικοινωνεί με τα εξωτερικά δεδομένα . Μια έξυπνη κάρτα επαφής έχει οκτώ επαφές , οι οποίες πρέπει να έχουν τυπικά μια επαφή με τις επαφές του αναγνώστη προκειμένου να μεταβιβάσουν τις πληροφορίες μεταξύ τους . Μια έξυπνη κάρτα μη επαφής χρησιμοποιεί την ίδια ράδιο-βασισμένη τεχνολογία με την κάρτα εγγύτητας , με εξαίρεση την ζώνη συχνοτήτων που χρησιμοποιεί . Οι έξυπνες κάρτες επιτρέπουν στο σύστημα ελέγχου πρόσβασης να αποθηκεύει τις πληροφορίες του χρήστη σε ένα πιστοποιητικό το οποίο φέρει ο χρήστης και το οποίο απαιτεί πάρα πολύ μνήμη από κάθε ελεγκτή.

Η επικύρωση διπλών παραγόντων χρησιμοποιεί συνδυασμό των μηχανισμών αυτών . Δηλαδή των έξυπνων καρτών και των USB
Η διαδικασία την επικύρωσης επιτυγχάνεται χρησιμοποιώντας τα παρακάτω :

1. Ένας μηχανισμό τον οποίο διαθέτουμε όπως μια έξυπνη κάρτα ή κάποιο USB .

Εικόνα 96 : Παράδειγμα μιας έξυπνης κάρτας.

Εικόνα 97 : Παράδειγμα USB.

2. Κάποιον κωδικό που γνωρίζουμε , όπως ένα προσωπικό αριθμό αναγνώρισης (PIN). Το PIN επιτρέπει στους χρήστες να έχουν πρόσβαση στο ψηφιακό πιστοποιητικό που αποθηκεύουμε στην έξυπνη κάρτα .

Και οι έξυπνες κάρτες και τα USB διαθέτουν ένα ενσωματωμένο τσιπ . Το τσιπ είναι στην ουσία ένας 32-bits μικροεπεξεργαστής και συνήθως περιέχει ένα 32KB ή 64KB ηλεκτρικά εξαλείψιμο προγραμματίσημο τσιπ (EPPROM) τυχαίας μνήμης προσπέλασης (RAM) που ενσωματώνεται στην έξυπνη κάρτα ή στο USB. Υπάρχουν επίσης έξυπνες κάρτες και USB διαθέσιμες σήμερα που μπορούν να περιέχουν μέχρι και 256KB RAM που είναι διαθέσιμα για την ασφαλή αποθήκευση στοιχείων .
Τα τσιπ αυτά περιέχουν ένα μικρό λειτουργικό σύστημα και μια μικρή μνήμη η οποία χρησιμοποιείται για την αποθήκευση πιστοποιητικών τα οποία χρησιμοποιούνται στην επικύρωση .
Το λειτουργικό σύστημα στα τσιπ διαφέρει από προμηθευτή σε προμηθευτή , και για αυτόν το λόγο θα πρέπει να διασφαλίσουμε ότι χρησιμοποιούμε κάποιον παροχέα υπηρεσίας κρυπτογράφησης CSP(Cryptographic Service Provider) στα Windows, ο οποίος να υποστηρίζει το λειτουργικό σύστημα του τσιπ.
Η λύση βασισμένη στην χρήση των τσιπς , έχει κάποια πλεονεκτήματα σε σύγκριση με τις άλλες πολυπαραγοντικές μεθόδους επικύρωσης, δεδομένου ότι μπορεί να χρησιμοποιηθεί για να αποθηκευτούν τα πιστοποιητικά τα οποία είναι απαραίτητα για την επικύρωση , τον προσδιορισμό και την υπογραφή . Όπως αναφέραμε και προηγουμένως , όλες οι πληροφορίες προστατεύονται από κάποιο PIN , το οποίο επιτρέπει στον χρήστη να έχει πρόσβαση στα δεδομένα τα οποία αποθηκεύονται στο τσιπ . Κάθε έξυπνη κάρτα ή USB μπορεί να ακολουθεί την δική της πολιτική η οποία καθορίζεται από την κατασκευαστική της εταιρεία και η οποία καθορίζει ακόμη πια μέθοδος λύσης θα ακολουθήσει σε οποιοδήποτε πρόβλημα και αν της παρουσιαστεί .
Για παράδειγμα , καθορίζεται ποιος είναι ο αριθμός των αποτυχημένων προσπαθειών εισόδου σε αυτά προτού αυτά κλειδωθούν ή διαγραφούν . Επίσης μπορούν αυτές οι πολιτικές να συνδυαστούν με το PIN , με αποτέλεσμα το PIN που θα χρησιμοποιήσουμε να μπορεί να είναι μικρότερο σε μήκος και με αποτέλεσμα πιο εύκολο στην απομνημόνευση του . Όλων αυτών των ειδών οι παράμετροι αποθηκεύονται στην έξυπνη κάρτα όταν αυτή παράγεται .

7.4.5.1.4 Smart cards Vs USB.

Όπως αναφέραμε μια από τις μεγάλες διαφορές μεταξύ της έξυπνης κάρτας και των USB είναι ο σχηματισμός που τους δίνουν οι εκάστοτε κατασκευαστές . Και οι δύο οι μηχανισμοί αυτοί σαν λύση στον πρόβλημα της επικύρωσης , μπορούν να μας λύσουν βασικές ανάγκες , έχουν πολλά πλεονεκτήματα αλλά και μειονεκτήματα .
Μια έξυπνη κάρτα μπορεί να χρησιμοποιηθεί για τον προσδιορισμό εικόνων , δεδομένου ότι μπορούμε να τυπώσουμε κάποια εικόνα και το όνομα αυτής στην κάρτα . Από την άλλη το USB μπορεί να χρησιμοποιηθεί περιλαμβάνοντας στην μνήμη του την αποθήκευση αρχείων και εγγράφων .
Και οι δύο οι συσκευές μπορούν εξίσου να χρησιμοποιηθούν για φυσική πρόσβαση ελέγχου , με τον δικό της τεχνικό τρόπο η κάθε μια . Η έξυπνη κάρτα μπορεί να περιλαμβάνει ένα κύκλωμα

τσιπ , μια μαγνητική λουρίδα , ένα bar code σε αντίθεση με μια συσκευή USB που μπορεί να έχει την ικανότητας της βιομετρικής υποστήριξης .
Υπάρχουν και άλλοι μορφολογικοί παράγοντες , όπως για παράδειγμα στα κινητά τηλέφωνα όπου η κάρτα Subscriber Identity Module (SIM) , μπορεί να χρησιμοποιηθεί για τον ίδιο σκοπό με την έξυπνη κάρτα ή με κάποιο USB έχει όμως διαφορετικό σχηματισμό .
Η έξυπνη κάρτα , απαιτεί επίσης συσκευή ανάγνωσης καρτών , ενώ σε αντίθεση το USB μπορεί αν χρησιμοποιήσει ,στην θέση της συσκευής ανάγνωσης ,την υπάρχουσα θύρα USB που διαθέτει ο υπολογιστής .
Στις μέρες μας , τέτοιοι μηχανισμοί ανάγνωσης καρτών (PC , Express Card, USB κ.α.) ενσωματώνονται στα interface των υπολογιστών μας και ιδιαίτερα στα notebooks . Θεωρούνται ως τυπικοί μηχανισμοί των Windows , ανεξαρτήτως του λειτουργικού συστήματος του τσιπ, και διαθέτουν έναν περιγραφέα και ένα προσδιοριστικό PnP.
Ομοίως και οι έξυπνες κάρτες και τα USB απαιτούν την εγκατάσταση των οδηγών συσκευής των Windows προκειμένου να λειτουργήσουν , τους οποίους οδηγούς πρέπει να κρατάνε ενημερωμένους , για λόγους καλύτερης αποδοτικότητας ιδιαίτερα κατά την διάρκεια της επικύρωσης διπλού παράγοντα.
Η επόμενη αξιοσημείωτη διαφορά που ενδέχεται να συναντήσουμε ανάμεσα στις δύο αυτές συσκευές , είναι η διαφορά που εμφανίζουν στο κόστος . Εκτός όμως από το κόστος, βασικό ρόλο στην επιλογή μπορεί να παίξουν και ψυχολογική παράγοντες .
Μια έξυπνη κάρτα και μια πιστωτική κάρτα , στην ουσία είναι το ίδιο πράγμα , στις μέρες μας βλέπουμε καθημερινά πάρα πολλούς ανθρώπους να έχουν στην κατοχή τους χρεωστικέ κάρτες , οι οποίες είναι βασισμένες στις νέες τεχνολογίες των τσιπ .Ακόμη πολλές επιχειρήσεις χρησιμοποιούνε τις έξυπνες αυτές κάρτες για διάφορες λειτουργίες, όπως την πρόσβαση του προσωπικού στα γραφεία ή την πληρωμή διαφόρων συναλλαγών μέσα στην εταιρεία όπως η αγορά μεσημεριανού κ.α.
Αυτό δείχνει ότι υπάρχει μια ευκολία στην χρήση αυτών των συσκευών και από ψυχολογική μεριά οι χρήστες εξοικειώνονται στην ιδέα να διαθέτουν τέτοιου είδους συσκευές και να τις έχουν μαζί τους χρησιμοποιώντας τες συνεχώς .

Από την άλλη πάλι , η επιλογή των χρηστών για χρήση των ειδικών αυτών συσκευών τσιπ επιφέρει στο προσκήνιο κάποια θέματα που πρέπει να τους απασχολήσουν . Τα θέματα αυτά αφορούν την συμβατότητα , την επέκταση , την διαχείριση και την χρησιμότητα αυτών .

1. **Συμβατότητα –Compatibility:** Θα πρέπει να διασφαλίσουμε ότι το OS του τσιπ είναι συμβατό με το CSP που θέλουμε να χρησιμοποιήσουμε . Το CSP είναι ένα υλικολογισμικό ανάμεσα στο OS του Chip και στα Windows το οποίο είναι επίσης αρμόδιο για την πολιτική ασφάλειας που εφαρμόζεται στο τσιπ.

2. **Διαχείριση- Management :** Εάν θα επιλέξουμε να χρησιμοποιήσουμε τις έξυπνες κάρτες και τα USB για χρήση πολλών χρηστών , θα πρέπει να σιγουρευτούμε ότι έχουμε επιλέξει ένα OS του τσιπ ,το οποίο να είναι συμβατό με το Card Management System (CMS) της επιλογής μας .

3. **Επεκτασιμότητα – Extensibility :** Θα πρέπει να βεβαιωθούμε ότι το OS του τσιπ μπορεί να χρησιμοποιηθεί από όλες τις απαιτούμενες εφαρμογές και από τις επικυρώσεις που απαιτούνται . Θ πρέπει να προνοήσουμε ότι στο μέλλον ίσως να έχουμε την ανάγκη για επιπλέον πιστοποιητικά στην έξυπνη κάρτα ή το USB μια υπογραφή ηλεκτρονικού ταχυδρομείου ή την κρυπτογράφηση του ή ακόμη και βιομετρικά δεδομένα . Για μεγαλύτερη ενημέρωση , καλό θα ήταν να ανατρέψουμε

σε εξωτερικές αναφορές προδιαγραφών καρτών πρόσβασης (CAC), οι οποίες χρησιμοποιούνται για την αποθήκευση πολλαπλών πληροφοριών του χρήστη .

4. **Δυνατότητα χρησιμοποίησης – Usability :** Τέλος θα πρέπει να σιγουρευτούμε ότι έχουμε επιλέξει και εφαρμόσει μια λύση βασισμένη στο τσιπ, η οποία είναι φιλική και πρακτική προς τον χρήστη . Μια από τις μεγαλύτερες προκλήσεις τον πολυπαραγοντικών λύσεων επικύρωσης είναι ότι οι άνθρωποι έχον την τάση είτε να ξεχνούν είτε νε χάνουν τις έξυπνες τους κάρτες είτε τις συσκευές USB τους , εάν δεν τις χρησιμοποιούν πολύ συχνά .

7.4.5.1.5 Βιομετρικά .

Τα ανθρώπινα αποτυπώματα , είναι ένα κοινός τύπος βιομετρικών στοιχείων που χρησιμοποιούνται στην διαδικασία της επικύρωσης
Και στις δύο περιπτώσεις οι προμηθευτές έχουν αρχίσει πλέον να προσθέτουν τους βιομετρικούς αναγνώστες στις συσκευές , παρέχοντας με αυτόν τον τρόπο πολλών παραγόντων επικύρωση .Οι χρήστες επικυρώνονται βιομετρικά , μέσω του δακτυλικού αποτυπώματος τους στην έξυπνη κάρτα ή το σημείο ασφάλειας και στην συνέχεια πρέπει να πληκτρολογήσουν τον απαραίτητο κωδικό πρόσβασης ή το PIN τους για να ανοίξουν με αυτόν τον τρόπο τον χώρο του πιστοποιητικού τους . Εντούτοις , ενώ αυτός ο τύπος επικύρωση είναι κατάλληλος σε περιορισμένες εφαρμογές , αυτή η λύση μπορεί να αποβεί απαράδεχτα αργή και συγκριτικά με τους άλλους τύπους ακριβή , ιδιαίτερα όταν περιλαμβάνεται ένας μεγάλος αριθμός χρηστών .
Επιπλέον είναι εξαιρετικά τρωτός σε επιθέσεις που επαναλαμβάνονται , καθώς μόλις συμβιβαστούν οι βιομετρικές πληροφορίες , μπορούν εύκολα να επαναληφθεί η διαδικασία της επίθεσης , εκτός και αν ο χρήστης είναι εντελώς πλέον ασφαλισμένος .
Για όλα τα βιομετρικά προσδιοριστικά , η πραγματική βιομετρική εικόνα ενός χρήστη δεν αποθηκεύεται και ελέγχεται σε σχέση με τις κρίσιμες πληροφορίες , αντίθετα ένα απόσπασμα αλγορίθμου ανίχνευσης της εικόνας αποθηκεύει το αποτέλεσμα ως μια σειρά στοιχείων .Η σύγκριση επομένως γίνεται μεταξύ δύο σειρών στοιχείων , και εάν υπάρχει ικανοποιητική κοινωνία πετυχαίνεται η πρόσβαση . Μπορούμε να εκτιμήσουμε την επιλογή του ποσού των δεδομένων που θα ταιριάζουν , και σε ποιό βαθμό ακρίβειας ελέγχοντας έτσι την αναλογία ακρίβειας/ ταχύτητας της βιομετρικής συσκευής .
Όλες οι βιομετρικές συσκευές, επομένως , δεν παρέχουν τις σαφείς εγγυήσεις της ταυτότητας αλλά μάλλον πιθανότητες αυτής , καθώς και όλες μπορούν να παρέχουν ψευδή και αρνητικά αποτελέσματα . Εάν ένα βιομετρικό σύστημα εφαρμόζεται σε έναν μεγάλο αριθμό χρηστών , το ποσοστό του λάθους της συσκευής μας ίσως να είναι μεγάλο , καθιστώντας έτσι το σύστημα μας μη πρακτικό για χρήση .

Τέλος , οι βιομετρικές πληροφορίες δεν μπορούν να αλλαχτούν ,έτσι ο βίο-προσδιοριστής μπορεί να είναι ψευδής . Είναι πιθανόν ότι , εάν τα βιομετρικά προσδιοριστικά γίνουν δεδομένα , οι περιπλοκότερες τεχνικές εξαπάτησης αυτών θα αναπτυχθούν .

PHONES

Μια νέα κατηγορία T-FA μηχανισμών είναι αυτοί , οι οποίοι μεταμορφώνουν το κινητό τηλέφωνο του χρήστη υπολογιστή σε μια συμβολική συσκευή που χρησιμοποιεί το μήνυμα SMS ή ένα διαλογικό τηλεφώνημα .
Δεδομένου ότι ο χρήστης επικοινωνεί τώρα πάνω από δύο κανάλια , το κινητό τηλέφωνο γίνεται ένας two-factor , διπλών καναλιών μηχανισμός επικύρωσης . Μερικές μέθοδοι τοποθετούν απλά ένα παραδοσιακό τηλεφώνημα στο τέλος , τηλεφώνημα του χρήστη , προτρέποντας τον χρήστη να πατήσει κάποιο πλήκτρο ή μια ακολουθίας κλειδιών . Αυτές οι λύσεις μπορούν να χρησιμοποιηθούν με οποιοδήποτε τηλέφωνο , όχι μόνο με τις κινητές συσκευές .
Αυτή όμως η μέθοδος , μπορεί να απλοποιήσει την επέκταση, να μειώσει τις λογιστικές δαπάνες και να αφαιρέσει την ανάγκη για ξεχωριστές συσκευές από τα σημεία .
Οι χρήστες μπορούν να εκμεταλλευτούν τα θετικά των υπηρεσιών κειμένων / στοιχείων ή τα κυψελοειδή όπως καλούνται πρακτικά . Επιπλέον , υπάρχει μια λανθάνουσα κατάσταση που περιλαμβάνεται με τις υπηρεσίες SMS ειδικά κατά την διάρκεια των μέγιστων περιόδων χρήσης αυτών , όπως στις διακοπές .
Υπάρχει μια νεώτερη μέθοδος χρησιμοποιώντας το κινητό ως επεξεργαστή και έχοντας τοποθετημένο το σημείο ασφάλειας στο ίδιο το κινητό ως JAVA ME client . Αυτή η μέθοδος δεν περιλαμβάνει την λανθάνουσα κατάσταση στοιχείων ή δεν αναλαμβάνει τις κρυμμένες δαπάνες για το τέλος του χρήστη .

Smart Cards

Οι έξυπνες κάρτες είναι περίπου στο μέγεθος των πιστωτικών καρτών . Μερικοί προμηθευτές προσφέρουν τις έξυπνες κάρτες , οι οποίες εκτελούν και την λειτουργία της εγγύτητας των καρτών και της επικύρωσης των δικτύων .
Οι χρήστες μπορούν να επικυρώσουν στο κτήριο μέσω της ανίχνευσης εγγύτητας και να παρεμβάλουν έπειτα την κάρτα στον υπολογιστή τους για παράγουν τα πιστοποιητικά σύνδεσης δικτύων . Μπορούν επίσης να χρησιμεύσουν ως διακριτικά ταυτότητας . Το μειονέκτημα είναι ότι η έξυπνη κάρτα είναι μια μεγαλύτερη συσκευή και έτσι ο αναγνώστης της έχει ένα επιπρόσθετο κόστος .
Επιπλέον πολλές τράπεζες και οικονομικά όργανα εφαρμόζουν την τεχνολογία CAP στην οποία ζευγάρια τραπεζικών έξυπνων καρτών εφαρμόζονται με έναν ανεξάρτητο και αποσυνδεμένο αναγνώστη καρτών .
Χρησιμοποιώντας την κάρτα , τον αναγνώστη και το PIN του ATM ως παράγοντες , ένα OTP παράγεται το οποίο και μπορεί έπειτα να χρησιμοποιηθεί αντί των κωδικών πρόσβασης .Η τεχνολογία αυτή προσφέρει υποστήριξη ενάντια στις MITM επιθέσεις , με την διευκόλυνση των στοιχείων συναλλαγής που υπογράφουν , όπως οι πληροφορίες από την συναλλαγή συμπεριλαμβάνονται στον υπολογισμό του OTP , αυτό είναι μια παρουσίαση αποδείξεων για να είναι ισχυρή η προστασία κατά την δημιουργίας των μεταφορών των τραπεζών ή άλλων οικονομικών συναλλαγών . Κατά την διάρκεια του χρόνου αυτού αυτή η μέθοδος T-FA είναι

διαθέσιμη και στο περιβάλλον του ηλεκτρονικού εμπορίου μέσω των τρισδιάστατων ασφαλών αρχιτεκτονικών οι οποίοι διαχειρίζονται από την MasterCard (Secure Code) και την VISA .

Universal Serial Bus

Κάθε σημείο USB έχει διαφορετικό παράγοντα μορφής , δεν μπορεί να ταιριάζει με οποιοδήποτε πορτοφόλι , αλλά μπορεί εύκολα να συνδέεται με ένα βασικό δακτυλίδι-κλειδί (key ring). Οι USB port είναι ένα τυποποιημένος εξοπλισμός στους σημερινούς ηλεκτρονικούς υπολογιστές και τα σημεία USB έχουν γενικά μια πολύ μεγαλύτερη ικανότητα αποθήκευσης για τα πιστοποιητικά σύνδεσης από τις έξυπνες κάρτες .

Άλλοι τύποι

Εικόνα 98 : Έμπιστα σημεία ασφάλειας Identity Guard OTP

Άλλοι πάλι κατασκευαστές προσφέρουν ένα σημείο κωδικού πρόσβασης ενός χρόνου (OTP). Αυτοί οι μηχανισμοί διαθέτουν μια LCD οθόνη που επιδεικνύει έναν ψευτοτυχαίο αριθμό αποτελούμενο από 6 ψηφία ή από περισσότερους αλφανουμερικούς χαρακτήρες (μερικές φορές είναι αριθμοί , άλλες πάλι φορές είναι συνδυασμοί γραμμάτων και αριθμών ανάλογα με τον προμηθευτή και το πρότυπο).
Αυτός ο ψευτοτυχαίος αριθμός αλλάζει σε προκαθορισμένα διαστήματα , συνήθως κάθε 60 δευτερόλεπτα, αλλά μπορεί επίσης να αλλάζει και σε άλλα χρονικά διαστήματα ή έπειτα από ένα γεγονός του χρήστη , όπως το να πατά ένα κουμπί ο χρήστης στο σημείο αυτό .
Τα σημεία που αλλάζουν μετά από έναν προκαθορισμένο χρόνο , καλούνται χρόνο-βασισμένα , και τα σημεία που απαιτούν ένα γεγονός των χρηστών αναφέρονται ως βασισμένα στην συχνότητα (δεδομένου ότι η αξία του διαστήματος είναι ο τρέχον αριθμός συχνοτήτων των γεγονότων των χρηστών , δηλαδή 1,2,3,4,κ.λπ).
Όταν αυτός ο ψευτοτυχαίο αριθμός συνδυάζεται με ένα PIN ή έναν κωδικό πρόσβασης , προκύπτουν pass code τα οποία θεωρούνται δύο παράγοντες της επικύρωσης (κάτι που εμείς γνωρίσουμε όπως το PIN/password , και κάτι που διαθέτουμε όπως το σημείο OTP). Υπάρχουν επίσης υβριδικά – σημεία που παρέχουν έναν συνδυασμό των ικανοτήτων των έξυπνων καρτών , των σημείων USB και των σημείων OTP.

7.4.5.1.6 Η τεχνολογία Bar code.

Τα Bar code είναι σειρά εναλλασσόμενων σκοτεινών και πιο ανοιχτόχρωμων λωρίδων , οι οποίες διαβάζονται από έναν οπτικό ανιχνευτή . Η οργάνωση και το πλάτος των γραμμών καθορίζονται από το πρωτόκολλο που είναι επιλεγμένο . Υπάρχουν πολλά και διαφορετικά πρωτόκολλα αλλά ο κωδικός 39 είναι ο δημοφιλέστερος στην βιομηχανίας της ασφάλειας . Σε μερικές περιπτώσεις τα στοιχεία που αντιπροσωπεύονται από τις σκοτεινές και ανοιχτόχρωμες λωρίδες , είναι επίσης τυπωμένα για να επιτρέπουν με αυτόν τον τρόπο στους χρήστες να μπορούν να διαβάσουν τον αριθμό χωρίς την παρουσία του οπτικού αναγνώστη .
Το πλεονέκτημα αυτής της τεχνολογίας είναι ότι είναι φθηνή, είναι εύκολο να παραχθεί το πιστοποιητικό και μπορεί εύκολα να εφαρμοστεί σε κάρτες και σε άλλα στοιχεία .Το μειονέκτημα της τεχνολογίας αυτής είναι ότι το γεγονός ότι είναι φθηνή και εύκολο να παραχθεί το πιστοποιητικό , την καθιστά ευαίσθητη στις απάτες , καθώς επίσης και ο οπτικός αναγνώστης μπορεί να εμφανίζει προβλήματα αξιοπιστίας.
Παράδειγμα προσπάθειας μείωσης των απατών που μπορεί να δεχτεί η τεχνολογία των bar code είναι αυτήν στην οποία χρησιμοποιούμε carbon βασισμένο στο μελάνι με το οποίο και καλύπτετε ο κώδικας και στην συνέχεια από πάνω του ακολουθεί μια σκούρα κόκκινη επικάλυψη . Αυτού του είδους το bar code μπορεί να διαβαστεί από ένα υπέρυθρο οπτικό αναγνώστη , και λόγω του τρόπου δημιουργίας του δεν μπορεί να αντιγραφτεί εύκολα από μια μηχανή αντιγράφων .

7.4.5.1.7 Η τεχνολογία Magnetic Stripe.

Η μαγνητική τεχνολογία λωρίδων , η οποία συχνά αποκαλείται και ως MAG-stripe , ονομάζεται έτσι λόγω της μαγνητικής ταινίας οξειδίων που είναι τοποθετημένη σε στρώματα σε μια κάρτα . Υπάρχουν τρείς διαδρομές των δεδομένων πάνω στην μαγνητική λωρίδα. Γενικά τα δεδομένα σε κάθε μια από τις τρείς διαδρομές ακολουθούν ένα συγκεκριμένο πρότυπο κωδικοποίησης , αλλά έχουν επίσης την δυνατότητα να κωδικοποιήσουν οποιοδήποτε σχήμα σε οποιαδήποτε διαδρομή .
Μια κάρτα MAG-stripe είναι φθηνή έναντι των άλλων τεχνολογιών των καρτών και είναι και εύκολη στο να προγραμματιστεί .Τα μαγνητικά λωρίδων έχουν την δυνατότητα να αποθηκεύουν περισσότερα στοιχεία από αυτά που μπορεί ένα bar code . Επίσης τα μαγνητικά λωρίδων είναι δυσκολότερο να παραχθούν από ότι ένα bar code. Η τεχνολογία ανάγνωσης και κωδικοποίησης όσο αφορά τα MAG-stripe είναι διαδεδομένη και εύκολο να αποκτηθεί , το γεγονός αυτό θα μπορούσε να χαρακτηριστεί και ως το κύριο μειονέκτημα τις τεχνολογίας αυτής .

7.4.6 Επικύρωση της νέας γενιάς

Η επικύρωση όπως προαναφέραμε είναι μια διαδικασία που ελέγχει την ταυτότητα κάποιου ατόμου (και δεν πρέπει να συγχέεται με την διαδικασία της έγκρισης η οποία δείχνει τι ένας χρήστης έχει άδεια να κάνει ,παρόλο που οι δύο αυτές διαδικασίες έχουν χρησιμοποιηθεί εναλλακτικά πολλές φορές).
Η επικύρωση είναι μια διαδικασία που έχει που έχει απασχολήσει τους IT επαγγελματίες για δεκαετίες . Οι κωδικοί πρόσβασης είναι ο βασικός παράγοντας – πρότυπο κατά την επικύρωση των χρηστών σε σχεδόν όλων των τύπων τα περιβάλλοντα εργασίας . Οι κωδικοί πρόσβασης

χρησιμοποιούνται για να κρατάνε τα προσωπικά μας δεδομένα ασφαλή και σε πολλές περιπτώσεις είναι ο μόνος διαθέσιμος έλεγχος που υπάρχει κατά των κακόβουλων λογισμικών που έχουν σαν στόχο τα δεδομένα μας .Κάθε φορά που δακτυλογραφείτε ο σωστός κωδικός πρόσβασης , χορηγείτε άμεσα στο εκάστοτε σύστημα το δικαίωμα της εισόδου πρόσβασης στον πόρο ή στους πόρους που επιθυμεί.
Με το πέρασμα των χρόνων το μέλημα όλων είναι η ασφάλεια μας να είναι όσο το δυνατόν ισχυρότερη . Οι επαγγελματίες ασφάλειας διαπίστωσαν ότι οι κωδικοί πρόσβασης είναι επιρρεπείς και εύκολα μπορεί να πραγματοποιηθεί ρωγμή σε αυτούς , αυτό συμβαίνει ιδιαίτερα σε περιπτώσεις που οι κωδικοί αυτοί είναι πολύ εύκολοι ,από την άλλη πάλι αν επιχειρήσουν οι χρήστες να τους δημιουργήσουν πιο σύνθετους αποτελούν πρόβλημα για αυτούς(είναι δύσκολο να συγκρατηθούν ή να ανακτηθούν από αυτούς) .

7.4.6.1 Ποιο είναι το πρόβλημα με τους κωδικούς πρόσβασης .

- Οι κωδικοί πρόσβασης μπορούν να αντιγραφτούν .
- Οι κωδικοί πρόσβασης μπορούν να αποκτηθούν από κακόβουλους χρήστες , παρακολουθώντας την επικοινωνία που γίνεται, μέσω των δεδομένων που μεταφέρονται στα καλώδια επικοινωνίας .
- Οι κωδικοί πρόσβασης μπορούν να αιχμαλωτιστούν τοπικά χρησιμοποιώντας εργαλεία της μορφής key loggers.
- Πάρα πολλοί χρήστες λόγο των πολλών κωδικών πρόσβασης που χρειάζεται να δακτυλογραφούν , χρησιμοποιούν ένα κωδικό πρόσβασης ίδιο για όλες τις εργασίες , γεγονός που κάνει πολύ ευάλωτο το σύστημα μας .
- SOX, HIPPA, GLB και οι άλλες απαιτήσεις διαμόρφωσης, διευκρινίζουν τώρα τον αυστηρό έλεγχο του κωδικού πρόσβασης ο οποίος δεν χρησιμοποιείται.

7.4.6.1.1 Λύσεις για να αντιμετωπίσουμε το πρόβλημα των ευάλωτων κωδικών πρόσβασης.

Το πρόβλημα των ευάλωτων κωδικών πρόσβασης μας είναι γνωστό , το θέμα είναι το τι μπορούμε να κάνουμε προκειμένου να κτίσουμε μια ισχυρότερη επικύρωση του οργανισμού ή της επιχείρησης μας .
Για να μην μπορούν να μας αντιγράψουν τον κωδικό πρόσβασης μας από, μια πρώτη λύση είναι η εφαρμογή της επικύρωσης τύπου διπλών παραγόντων .
Για να μην υποκλέπτεται ο κωδικός πρόσβασης μας μέσω της παρακολούθησης των συνομιλιών μας , η λύση είναι ένας κρυπτογραφημένος κωδικός ή θα μπορούσαμε να κρυπτογραφούμε το δίκτυό μας και έπειτα το διαδίκτυο , αλλά επειδή αυτό πρόκειται για μια μακροπρόθεσμη εργασία , θα μας βοηθούσε η χρήση ενός onetime κωδικός πρόσβασης .
Η ¨αιχμαλώτιση¨ του τοπικού κωδικού πρόσβασης μας είναι δύσκολο να ανατρέπει ιδιαίτερα σε περιπτώσεις όπως γίνεται χρήση των physical key loggers , τα οποία και είναι διαθέσιμα στις μέρες μας .Είναι πολύ δύσκολο να ανιχνευτούν οι επιτιθέμενοι , χρησιμοποιώντας λογισμικά ανίχνευσης και τις περισσότερες περιπτώσεις είναι πολύ δύσκολο να σημειωθούν , εκτός και αν οι λογιστικές λεπτομέρειες των ελέγχων ασφαλείας του υλικού είναι ενεργοποιημένοι . Και σε αυτήν την περίπτωση οι onetime κωδικοί αποτελούν μια εύκολή λύση .

7.4.6.2 Onetime Passwords

Τα **Onetime passwords ,** είναι κωδικοί οι εκδίδονται και χρησιμοποιούνται μια μόνο φορά , οι κωδικοί αυτοί παράγονται συχνά από συμβολικές συσκευές οι οποίες είναι συγχρονισμένες με κάποιον κεντρικό υπολογιστή . Ο κεντρικός υπολογιστής προκαλεί τον χρήστη να του παρέχει έναν κωδικό πρόσβασης και ο χρήστης χρησιμοποιώντας αυτό το συμβολικό σημείο παράγει τον κωδικό αυτό. Αυτός ο onetime κωδικός πρόσβασης , χρησιμοποιείται έπειτα για να επικυρώσει , ως κομμάτι ενός κανονικού μηχανισμού ασφάλειας, τα κανονικά πιστοποιητικά , το όνομα χρήστη και τον κωδικό πρόσβασης .

7.4.6.3 Single Sing On

Τα πολλαπλά συστήματα που πρέπει να προσεγγίσουμε ,μας αναγκάζουν να παρέχουμε πολλά και διαφορετικά πιστοποιητικά σε κάθε εφαρμογή που επιθυμούμε να εκτελέσουμε. Για τον λόγο αυτό οδηγούμαστε στην εφαρμογή των συστημάτων Single Sing On (SSO). Αυτά τα SSO συστήματα , απομονώνουν τα πιστοποιητικά μας , τα οποία στη συνέχεια μετατρέπουν σε μοναδικές και σύνθετες σειρές από string-συμβολοσειρές οι οποίες και στέλνονται αντί αυτών κάθε φορά που απαιτούνται τα πιστοποιητικά .
Τα πιστοποιητικά αυτά αποθηκεύονται κυρίως στον κεντρικό υπολογιστή του SSO όπως και τα τοπικά , σε μια κρυπτογραφημένη μορφή . Μαζί με τον μηχανισμό της επικύρωσης διπλού παράγοντα ο μηχανισμός SSO βοηθάει να κτίσουμε ένα πιο ασφαλέστερο μηχανισμό επικύρωσης .

7.4.6.3.1 Γιατί να χρησιμοποιούμε τον μηχανισμό SSO;

Ο μηχανισμός Single Sing On , απλοποιεί την πρόσβαση μας στα συστήματα ελαχιστοποιώντας τον αριθμό των πιστοποιητικών που ένας χρήστης πρέπει να θυμηθεί . Ένα ακόμη θετικό στοιχείο είναι ότι έχουμε εξοικονόμηση χρημάτων με την χρησιμοποίηση του SSO , η χρήση του μηχανισμού αυτού μας απαιτεί την ιδιαίτερη προσοχή μας και ιδιαίτερα όταν δεν είμαστε έμπειροι χρήστες .
Ένα σωστά ανεπτυγμένο SSO συνεπάγεται εξοικονόμηση χρόνου και χρημάτων , άμεσο μέλημα όλων των επιχειρήσεων.

7.4.6.4 Τι είναι ο Ανοικτός Καθορισμός Διεπαφών Υπηρεσιών Επικύρωσης (Authentication Open Service Interface Definition-OSID) ;

Ο Ανοικτός Καθορισμός Διεπαφών Υπηρεσιών Επικύρωσης (OSID) είναι μιας ανοικτής πρωτοβουλίας γνώση προδιαγραφής (τεχνικού προτύπου), η οποία υποστηρίζει την επίκληση μιας μεθόδου επικύρωσης . Τα OSIDs είναι προγραμματιστικές διεπαφές που περιλαμβάνουν μια προσανατολισμένη υπηρεσία αρχιτεκτονικής για το σχεδιασμό και την οικοδόμηση του επαναχρησιμοποιήσιμου και διαλειτουργικού λογισμικού .
Η χρήση αυτής της λειτουργίας είναι η συλλογή οποιασδήποτε πληροφορίας η οποίας είναι κατάλληλη για την ορθή εκτέλεση μιας επικύρωσης . Αυτή η λειτουργία υποστηρίζει την δοκιμή ,

εάν κάποιος χρήστης επικυρώνεται , επιστρέφοντας την ταυτότητα Agent που αντιστοιχεί στον επικυρωμένο χρήστη .
Τα OSIDs μπορούν τέλος , να αλληλεπιδράσουν με τις πληροφορίες και τους πόρους ανεξαρτήτου μορφής ή ελέγχου πρόσβασης και αν αυτά διαθέτουν .Η Επικύρωση , ο Agent και η Έγκριση μιας εργασίας μαζί , είναι εργασίας που εξασφαλίζουν ότι οι αλληλεπιδράσεις είναι αποτελέσματα αιτήσεων του χρήστη , και η έγκριση εκθέτει τι ο προσδιορισμένος χρήστης είναι σε θέση να κάνει .

7.4.6.5 Biometrics.

Καλό θα ήταν στο σημείο αυτό να αναλύσουμε τον ορισμό Biometrics , μηχανισμοί για τους οποίους αναφερθήκαμε σε προηγούμενες παραγράφους και σχετίζονται με την διαδικασία επικύρωσης κάποιου χρήστη .
Με τον όρο Biometrics , αναφερόμαστε σε δύο διαφορετικούς τομείς μελέτης και εφαρμογών. Ο πρώτος τομέας ο οποίος είναι και ο παλιότερος είναι αυτός που χρησιμοποιείται για τις βιολογικές μελέτες , αναφέρεται στην συλλογή , σύνθεση , ανάλυση και διαχείριση των ποσοτικών στοιχείων που συλλέγονται για κάποιο τομέα όπως είναι η δασονομία η ανθρωπολογία κα και τα στοιχεία αυτών μελετούνται και αντιμετωπίζονται ως βιολογικές στατιστικές.

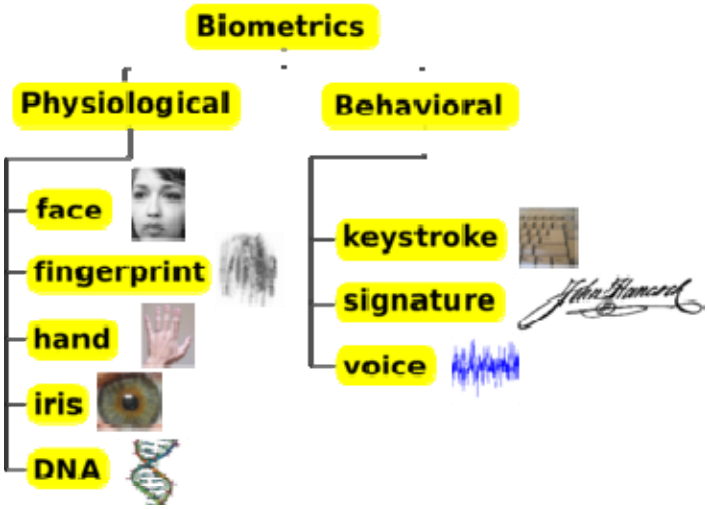
Πιο πρόσφατες αναφορές ,διευρύνουν την έννοια του ορισμού αυτού , με τον ορισμό αυτό περιλαμβάνουν την μεμονωμένη μελέτη ανθρώπων , βασιζόμενοι στα χαρακτηριστικά και φυσικά γνωρίσματα των ατόμων .
Μερικοί ερευνητές και επιστήμονες έχουν δημιουργήσει τον όρο behaviometrics τον οποίο αποδίδουν στην βιομετρική συμπεριφορά των ατόμων , όπως ο ρυθμός δακτυλογράφησης ή οι χειρονομίες του ποντικιού , η ανάλυση των οποίων μπορεί να γίνει χωρίς διακοπή η οποιαδήποτε παρεμπόδιση από οποιαδήποτε δραστηριότητα των χρηστών .
Η βιομετρική χρησιμοποιείται για να προσδιορίσει το δείγμα εισαγωγής , το οποίο συγκρίνεται με ένα πρότυπο , και χρησιμοποιείται σε ορισμένες περιπτώσεις για να προσδιορίσει συγκεκριμένους ανθρώπους από ορισμένα χαρακτηριστικά :

- **Βασισμένα στην κατοχή :** Το να κατέχει και να χρησιμοποιεί ο χρήστης κάποιο συγκεκριμένο σημείο, όπως μια ετικέτα ασφαλείας ή μια κάρτα .

- **Βασισμένα στην γνώση :** Το αν γνωρίζει ο χρήστης κάποιον κωδικό ή κωδικό πρόσβασης .

Τα τυποποιημένα συστήματα επικύρωσης χρησιμοποιούν συχνά πολλαπλές εισαγωγές δειγμάτων , για την αποπεράτωση διαδικασιών επικύρωσης . Αυτό ενισχύει την ασφάλεια αφού απαιτούνται πολλαπλά διαφορετικά δείγματα όπως οι ετικέτες ασφάλειας και οι κωδικοί .

7.4.6.5.1 Γνωστά ανθρώπινα βιομετρικά χαρακτηριστικά.



Σχ. Ταξινόμηση μερικών βιομετρικών γνωρισμάτων.

Τα βιομετρικά χαρακτηριστικά διαιρούνται σε δύο κύριες κατηγορίες , οι οποίες φαίνονται στον παραπάνω σχήμα .

- **Φυσιολογικά :** Αυτού του είδους τα βιομετρικά χαρακτηριστικά συσχετίζονται με την μορφή του ανθρώπινου σώματος . Είναι τα παλαιότερα σε χρονολογία γνωρίσματα τα οποία έχουν χρησιμοποιηθεί . Παράδειγμα αυτών είναι τα δακτυλικά αποτυπώματα , η αναγνώριση προσώπου , η γεωμετρία χεριών η αναγνώριση ιρίδων κ.α. Τα βιομετρικά αυτά συστήματα βασίζονται στην χρήση του λειτουργικού transcranial Doppler (fTCD) και της λειτουργικής transcranial φασματοσκοπίας Doppler (fTCDS) τα οποία παίρνουν τις απαντήσεις του εγκεφάλου και τις συγκρίνουν , με σκοπό να τις ταιριάξουν με ένα σύνολο στόχων , ή με κάποιο χαρακτηριστικό ενός προσώπου τα οποία είναι αποθηκευμένα σε μια βάση δεδομένων υπολογιστών .

- **Συμπεριφοριστικά :** Αυτού του είδους τα βιομετρικά χαρακτηριστικά συσχετίζονται με την συμπεριφορά ενός ατόμου . Το πρώτο χαρακτηριστικό τέτοιου είδους που χρησιμοποιείται ευρέως είναι η υπογραφή . Πιο σύγχρονες προσεγγίσεις των χαρακτηριστικών αυτών είναι δυναμική πληκτρολόγηση (keystroke dynamics) και η αναγνώριση φωνής . Η φωνή πολλές φορές χαρακτηρίζεται και ως φυσιολογικό βιομετρικό χαρακτηριστικό , η μελέτη όμως του τρόπου που ένα πρόσωπο μιλά ,συνήθως ταξινομείται ως συμπεριφοριστικό χαρακτηριστικό .

Τέλος τα τελευταία χρόνια αναπτύσσονται και άλλες βιομετρικές στρατηγικές που βασίζονται στον βηματισμό (τρόπος) , στον αμφιβληστροειδή , στο σχηματισμό των χεριών , ή στον σχηματισμό των αυτιών ή του προσώπου , στο DNA και γενικά σε πολλά ανθρώπινα χαρακτηριστικά.

7.4.6.5.2 Σύγκριση των διαφόρων βιομετρικών τεχνολογιών

Στην παράγραφο αυτή θα κατανοήσουμε πως είναι εφικτό να καταλάβουμε εάν κάποιο ανθρώπινο χαρακτηριστικό μπορούμε να το χρησιμοποιήσουμε από βιομετρικής άποψης ή όχι . Οι παράγοντες που μας οδηγούν στο παραπάνω συμπέρασμα , έχουν να κάνουν με έναν αριθμό από παραμέτρους . Οι παράμετροι αυτοί μας βοηθάνε ακόμη να αξιολογήσουμε και να συγκρίνουμε τις βιομετρικές μεθόδους μεταξύ τους , προκειμένου να επιλέξουμε αυτήν η οποία θα μας εξυπηρετήσει καλύτερα και με μεγαλύτερη ασφάλεια :

- **Καθολικότητα :** Κάθε άτομο θα πρέπει να έχει το χαρακτηριστικό .
- **Μοναδικότητα :** Είναι ο τρόπος με τον οποίο η βιομετρική τεχνολογία χωρίζει το κάθε άτομο από οποιοδήποτε άλλο .
- **Μονιμότητα :** Αξιολογεί πόσο καλά αντέχει(πόσο δηλαδή αποδοτική είναι) η βιομετρική τεχνολογία στο πέρασμα των χρόνων .
- **Περισυλλογή :**Μετρά πόσο εύκολη είναι η περισυλλογή των στοιχείων .
- **Απόδοση :** Ακρίβεια , ταχύτητα ,πόσο ευρέως χρησιμοποιημένη είναι κ.α.
- **Αποδοχή :**Βαθμός αποδοχής – έγκρισης μιας τεχνολογίας .
- **Παράκαμψη** :Ευκολία χρήσης ενός υποκατάστατου προγράμματος .

Ο πίνακας που ακολουθεί παρουσιάζει συγκριτικά τις υπάρχοντες βιομετρικές τεχνικές με βάση τις παραμέτρους που προαναφέραμε.

Πίνακας 8: Σύγκρισης των βιομετρικών τεχνικών

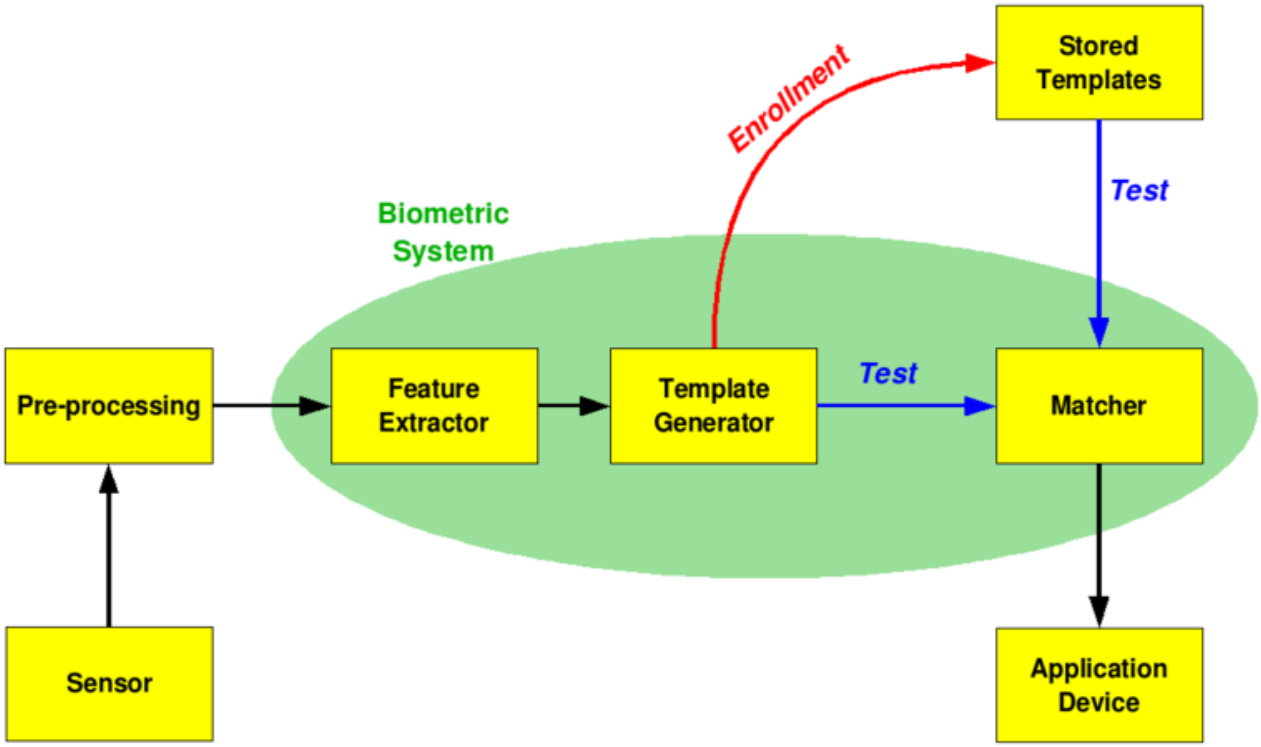
Βιομετρικά χαρακτηριστικά	**Καθολικότητα**	**Μοναδικότητα**	**Μονιμότητα**	**Περισυλλογή**	**Απόδοση**	**Αποδοχή**	**Παράκαμψη**
Πρόσωπο	H	L	M	H	L	H	L
Αποτυπώματα	M	H	H	M	H	M	H
Γεωμετρία Χεριών	M	M	M	H	M	M	M
Δυναμική πληκτρολογίσματος	L	L	L	M	L	M	M
Φλέβες χεριών	M	M	M	M	M	M	H
Ίριδα ματιών	H	H	H	M	H	L	H
Ανίχνευση αμφιβληστροειδή	H	H	M	L	H	L	H
Υπογραφή	L	L	L	H	L	H	L
Φωνή	M	L	L	M	L	H	L

Θερμογραφία προσώπου	H	H	L	H	M	H	H
Ανίχνευση μυρωδιάς	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Βηματισμός	M	L	L	H	L	H	M

H= High, M=Medium, L=Low.

7.4.6.5.3 Βιομετρικά συστήματα .

Στο κομμάτι αυτό θα αναφερθούμε στον τρόπο λειτουργίας των βιομετρικών συστημάτων . Στην εικόνα που ακολουθεί παρουσιάζεται ένα απλό διάγραμμα φραγμών ενός βιομετρικού συστήματος . Όταν ένα τέτοιου είδους σύστημα είναι δικτυωμένο μαζί με την τεχνολογία των τηλεπικοινωνιών , τα βιομετρικά του συστήματα μετατρέπονται σε τηλεβιομετρικά συστήματα .



Εικόνα 99: Περιγραφή βιομετρικών συστημάτων .

Οι κύριες εργασίες που ένα σύστημα μπορεί να εκτελέσει , όσο αφορά τα βιομετρικά συστήματα , είναι η **εγγραφή** και η **δοκιμή** . Κατά την εγγραφή , οι βιομετρικές πληροφορίες από ένα άτομο αποθηκεύονται , εδώ πρέπει να σημειώσουμε ότι σε περίπτωση που επιθυμούμε το βιομετρικό σύστημα μας να είναι ισχυρό , η αποθήκευση και η ανάκτηση αυτών των συστημάτων θα πρέπει να εξασφαλίζεται από τα ίδια τα συστήματα και να είναι ασφαλής.
Με βάση λοιπόν και του σχήματος , παρατηρούμε ότι ο πρώτος φραγμός (sensor) είναι μεταξύ του πραγματικού κόσμου και του συστήματος μας , θα πρέπει ο αισθητήρας αυτός να αποκτήσει όλα τα απαραίτητα στοιχεία για να συνεχίσει η εκτέλεση της εργασίας . Τις περισσότερες φορές είναι ένα σύστημα απόκτησης εικόνας , το οποίο όμως έχει την ικανότητα να μετατρέπεται ανάλογα με τα εκάστοτε επιθυμητά χαρακτηριστικά . Ο δεύτερος φραγμός εκτελεί όλη την απαραίτητη προεπεξεργασία , η δουλειά του είναι να αφαιρεί όλα τα χειροποίητα αντικείμενα από τον αισθητήρα ,να ενισχύει το σήμα εισόδου (αφαιρώντας τον θόρυβο) , να χρησιμοποιεί κάποιου είδους κανονικοποίηση κ.α. . Στον τρίτο φραγμό , εξάγονται τα χαρακτηριστικά γνωρίσματα που απαιτούνται . Αυτό το βήμα αποτελεί σημαντικό κομμάτι όλης της διαδικασίας , καθώς πρέπει να εξαγχθεί ο βέλτιστος τρόπος και τα σωστά χαρακτηριστικά γνωρίσματα.
Ένα διάνυσμα αριθμών ή μια εικόνα, με ιδιαίτερες ιδιότητες χρησιμοποιείται προκειμένου να δημιουργηθεί ένα πρότυπο . Το πρότυπο είναι σύνθεση όλων των χαρακτηριστικών που εξάγονται από την πηγή . Εάν η διαδικασία της εγγραφής εκτελείται το πρότυπο αυτό , αποθηκεύεται απλά κάπου (ή σε μια κάρτα ή σε μια βάση δεδομένων ή και στα δύο). Στην περίπτωση τώρα που μια φάση –διαδικασία που μοιάζει εκτελείται , το αποκτηθέν πρότυπο περνά από έναν μηχανισμό (matcher) , ο οποίος το συγκρίνει με τα άλλα υπάρχοντα πρότυπα , υπολογίζοντας τις διαφορές που έχουν αυτά μεταξύ τους χρησιμοποιώντας κάποιον αλγόριθμο (πχ Hamming Distance). Το πρόγραμμα ταυτοποίησης θα αναλύσει το πρότυπο σε σχέση με το σήμα

εισόδου . Το αποτέλεσμα θα είναι στην συνέχεια η έξοδος για οποιονδήποτε διευκρινισμένο χρήστη ή σκοπό (για παράδειγμα η είσοδος σε μια απαγορευμένη περιοχή).

7.4.6.5.4 Λειτουργίες των βιομετρικών συστημάτων.

Τα βιομετρικά συστήματα μπορούν να προβούν σε δύο λειτουργίες . Στην **Επαλήθευση** και στον **Προσδιορισμό** :

- **Επαλήθευση:** Στην λειτουργία αυτή επικυρώνεται ο χρήστης με την χρήση κάποια έξυπνης κάρτας, ενός ονόματος χρήστη ή ενός αριθμού ταυτότητας ID. Το βιομετρικό πρότυπο που συλλαμβάνεται συγκρίνεται, με αυτό το πρότυπο που είναι αποθηκευμένο για τον εγγεγραμμένο χρήστη , και βρίσκεται είτε σε μια έξυπνη κάρτα είτε σε μια βάση δεδομένων και επαληθεύεται .

- **Προσδιορισμός:** Στην λειτουργία αυτή επικυρώνονται οι χρήστες μόνο από το βιομετρικό χαρακτηριστικό , χωρίς την χρήση της έξυπνης κάρτας ή του ονόματος χρήστη ή του αριθμού ταυτότητας . Το βιομετρικό πρότυπο συγκρίνεται με όλα τα αρχεία μέσα στην βάση δεδομένων και αυτό το αρχείο το οποίο εμφανίζεται να αντιστοιχεί πιο κοντά στο πρότυπό του χρήστη , επιστρέφεται ως αποτέλεσμα . Η πιο στενή αντιστοιχία μέσα στο κατώτερο όριο κρίνει το άτομο που επικυρώνεται .

7.4.6.6 Τι είναι η επικύρωση πολλών παραγόντων ;

Η επικύρωση πολλών παραγόντων ή η ισχυρή επικύρωση όπως αλλιώς αναφέρεται ,τυπικά αποτελείται από δύο ή περισσότερους μηχανισμούς επικύρωσης . Η ισχυρή επικύρωση μπορεί να παρομοιαστεί με τις πολλές κλειδαριές σε μια πόρτα σπιτιού .
Πολλές κλειδαριές συνεπάγεται επιπλέον ασφάλεια . Τα επίπεδα ασφαλείας που διατίθενται όμως από την επικύρωση αυτή μας παρέχει πολλαπλά επίπεδα ασφάλειας τα οποία δεν είναι όλα αποτελεσματικά για εμάς αλλά μόνο σε ορισμένες περιπτώσεις εμφανίζονται απόλυτα αποτελεσματικά . Η λεπτομερής περιγραφή , από την άλλη είναι αναγκαία για να μπορεί να σχεδιαστεί προσεχτικά βήμα βήμα και να είναι αποτελεσματική η χρήση της επικύρωσης πολλών παραγόντων .
Από την αρχή μέχρι και τα τελευταία χρόνια , οι κωδικοί πρόσβασης αποτελούσαν τους πιο γνωστούς σε προτίμηση μηχανισμούς επικύρωσης για την πρόσβασή μας στα διάφορα συστήματα και στα ευαίσθητα δεδομένα μας. Οι απαιτήσεις όμως των χρηστών για υψηλότερη

ασφάλεια και ευκολία , χωρίς να αυξάνεται η πολυπλοκότητα τους , μας οδήγησαν στην αναζήτηση νέων μεθόδων επικύρωσης .
Επιστημονικά ήταν αποδεδειγμένο ότι ο μέσος άνθρωπος είχε την δυνατότητα να αποθηκεύσει επτά κομμάτια πληροφορίας την φορά με απόκλιση πάνω κάτω δύο . Άλλοι πάλι θεωρούν ότι ένας μέσος άνθρωπος μπορεί να αποθηκεύσει και να επεξεργάζεται μέχρι πέντε κομμάτια την φορά . Και στις δύο περιπτώσεις το συμπέρασμα είναι το ίδιο ότι οι κωδικοί πρόσβασης θα πρέπει να έχουν σχετικά μικρό μήκος και να μην είναι πολύπλοκοι για να είναι ευκολόχρηστοί για τους χρήστες , ταυτόχρονά όμως γίνονται πιο εύκολη η εκμετάλλευσής τους από κακόβουλους χρήστες .
Αναφέρεται ακόμη συχνά ότι η πολυπλοκότητα είναι μια από τις μεγαλύτερες απειλές της ασφάλειας . Μια από τις περιοχές οπού αυτό το γεγονός γίνεται αντιληπτό είναι όταν απαιτείται από τους χρήστες και τους διαχειριστές να ακολουθήσουν μια σύνθετη πολιτική κωδικού πρόσβασης .

Οι κωδικοί πρόσβασης ως μοναδικοί μηχανισμοί επικύρωσης είναι καλοί όσο αφορά κωδικούς με μήκος πάνω από δεκαπέντε χαρακτήρες και οι οποίοι να μην αποτελούνται μόνο από αγγλικούς χαρακτήρες αλλά και από άλλα στοιχεία όπως αριθμούς ή σημεία στίξης κα. Παράδειγμα τέτοιων κωδικών είναι οι φράσεις πρόσβασης , οι οποίες είναι μακριές σε μήκος κωδικοί που οι χρήστες πρέπει να θυμούνται για μεγάλη χρονική περίοδος . Αυτές οι φράσεις εξασφαλίζουν οι περισσότερες από τις τοξοειδής επιθέσεις ακόμη και οι 8-bit να αποτυγχάνουν , λόγω της προστιθέμενης πολυπλοκότητας που οι ¨ξένοι ¨ αυτοί χαρακτήρες προσθέτουν .
Μέχρι την εποχή των Windows 2000 , το μήκος των κωδικών πρόσβασης έφτανε τους 127 χαρακτήρες . Ο λόγος εντούτοις που οι κωδικοί πρόσβασης ως μοναδικοί μηχανισμοί επικύρωσης είναι ανεπαρκείς είναι επειδή οι χρήστες είναι κακοί στην απομνημόνευση ¨καλών¨ κωδικών ασφάλειας .
Ευτυχώς , υπάρχουν και άλλες λύσεις ασφάλειας που μας βοηθούν να ενισχύσουμε την ασφάλεια μας οι οποίες εισάγουν την ευκολία στην χρησιμοποίηση ενός σύντομου και ευκολομνημόνευτου κωδικού πρόσβασης .

7.4.7 Αναλυτική περιγραφή του μηχανισμού Επικύρωσης.

Η επικύρωση είναι μια βασική πτυχή απόδοσης ταυτότητας βασισμένη στην εμπιστοσύνη .Παρέχει κωδικοποιημένη ασφάλεια μιας ταυτότητας από μια οντότητα σε μια άλλη . Υπάρχουν διαφόρων τύπων επικυρώσεις ,αρχικά θα μελετήσουμε δύο βασικούς τύπους , αυτούς της **βασικής επικύρωσης** και στην συνέχεια την **επικύρωση αφομοιώσεων** .

7.4.7.1 Βασική Επικύρωση .

Όπως φαίνεται και από το όνομα , ο πρώτος αυτός τύπος επικύρωσης , είναι η πιο απλούστερη μέθοδος επικύρωσης καθώς και η πιο πολυχρησιμοποιούμενη.

7.4.7.1.1 Πως λειτουργεί η βασική επικύρωση .

Όταν κάποιος πόρος του συστήματος μας προστατεύεται από την βασική επικύρωση ακλουθείτε η παρακάτω διαδικασία ασφάλειας. Αρχικά στέλνεται μια αίτηση επικύρωσης η οποία εμφανίζει την επιγραφή ¨a401 επικύρωση που απαιτείται¨, και η οποία στέλνεται στον χρήστη για να τον ειδοποιήσει να παράσχει να απαραίτητα πιστοποιητικά με σκοπό να του επιτραπεί η πρόσβαση στον πόρο .
Με την λήψη της αίτησης αυτής η μηχανή αναζήτησης του χρήστη , εάν υποστηρίζει την βασική επικύρωση , θα του ζητήσει έναν κωδικό και ένα όνομα χρήστη τα οποία και θα στείλει στον κεντρικό υπολογιστή . Εάν ο κωδικός και το όνομα χρήστη είναι σωστά θα χορηγείται πρόσβαση στον πόρο για τον συγκεκριμένο χρήστη, και επειδή το πρωτόκολλο HTTP είναι άνευ υπηκοότητας , κάθε αίτηση είτε προέρχεται από έναν χρήστη είτε από τον κεντρικό υπολογιστή αντιμετωπίζεται με τον ίδιο τρόπο . Δηλαδή σε αντίστοιχη περίπτωση που κάποιος πόρος ζητηθεί από τον κεντρικό υπολογιστή , θα πρέπει και αυτός με την σειρά του να παρέχει τα σωστά πιστοποιητικά επικύρωσης για να του παρασχεθεί πρόσβαση στο πόρο .

Οι λεπτομέρειες των διαδικασιών αυτών υλοποιούνται , χωρίς να γίνονται αντιληπτές από τους χρήστες , από την αντίστοιχη μηχανή αναζήτησης . Το μόνο μέλημα των χρηστών είναι να πληκτρολογήσουν τον κωδικό πρόσβασης και το όνομα χρήστη .
Μαζί με την αίτηση απάντηση , εκτός από την άδεια πρόσβασης παρέχονται και άλλες πληροφορίες στον χρήστη . Υπάρχουν περιπτώσεις όπου στις πληροφορίες αυτές εμπεριέχεται ένα όνομα που συνδέεται με την προστατευμένη ζώνη του Ιστοχώρου . Αυτό το όνομα καλείται **σφαίρα** ή αλλιώς **όνομα επικύρωσης** .
Συνοπτικά , λοιπόν με βάση αυτά που αναφέραμε παραπάνω η βασική επικύρωση απαιτεί την παροχή από τον χρήστη κάποιου κωδικού και κάποιου ονόματος χρήστη . Η μέθοδος επικύρωσης αυτή , δεν χρειάζεται κάποιον εξειδικευμένο browser προκειμένου να λειτουργήσει , όλοι οι βασικοί browser την υποστηρίζουν . Ακόμη δουλεύει σε συνεργασία με το firewall και τους proxy server (για αυτούς τους λόγους είναι πολύ χρήσιμη όταν επιθυμούμε να περιορίσουμε σε κοινόχρηστους υπολογιστές ,την πρόσβαση στα περιεχόμενα των υπολογιστών αυτών ,σε συγκεκριμένα μέλη και όχι σε όλα).
Στην συνέχεια θα αναφέρουμε κάποια βήματα διαμόρφωσης που πρέπει να προηγηθούν προκειμένου ένας πόρος μας να προστατεύεται από επικύρωση βασικού τύπου .Τα βήματα που πρέπει να ακολουθηθούν προκειμένου να ολοκληρωθεί η διαμόρφωση αυτή είναι δύο ή τρία εξαρτάται από αυτό που ακριβώς που θέλουμε να κάνουμε .

1. Αρχικά δημιουργούμε ένα αρχείο κωδικού πρόσβασης .
2. Στην συνέχεια θέτουμε τον τύπο της διαμόρφωσης που θα εφαρμόσουμε στο αρχείο του κωδικού πρόσβασης .
3. Τέλος , προαιρετικά , δημιουργούμε ένα αρχείο ομάδας.

7.4.7.1.2 Πως δημιουργούμε ένα αρχείο κωδικού πρόσβασης .

Όπως προαναφέραμε σε κάθε χρήστη αντιστοιχεί κάποιος κωδικός πρόσβασης και κάποιο όνομα χρήστη , τα οποία και πρέπει να παρέχει όποτε του ζητηθούν σαν αποδεικτικά στοιχεία της ταυτότητάς του .

Προκειμένου , λοιπόν να καθοριστεί εάν ένας συγκεκριμένος συνδυασμός ονόματος χρήστη και κωδικού πρόσβασης , ανήκει σε κάποιον χρήστη , θα πρέπει να συγκριθούν τα στοιχεία αυτά με κάποια επιτακτική λίστα κωδικών πρόσβασης και ονομάτων χρήστη .
Επειδή το αρχείο πρόσβασης περιέχει τις ευαίσθητες πληροφορίες του χρήστη , θα πρέπει να αποθηκευτεί κάπου απομονωμένα και έξω από τον κατάλογο των εγγραφών αν και δεδομένου ότι τα αρχεία των κωδικών πρόσβασης κρυπτογραφούνται, παρόλα αυτά για την ενίσχυση της ασφάλειας τα αρχεία αυτά έχουν άλλο προορισμό αποθήκευσης από αυτόν των εγγραφών .
Οι κατασκευαστές ενθαρρύνουν τους χρήστες τους να χρησιμοποιούν ένα διαφορετικό κωδικό πρόσβασης για τον Ιστοχώρο του από ότι για τα άλλα πιο ουσιαστικά πράγματα . Για παράδειγμα οι πιο εξειδικευμένοι χρήστες τείνουν να χρησιμοποιούν δύο κωδικούς πρόσβασης , έναν για τα πιο σημαντικά πράγματα τους , όπως η σύνδεση στον υπολογιστή του γραφείου τους ή για τον τραπεζικό λογαριασμό τους , και έναν άλλο κωδικό για τα λιγότερο σημαντικά και ευαίσθητα πράγματα τους , των οποίων ο συμβιβασμός από κακόβουλα λογισμικά θα ήταν λιγότερο σοβαρός .
Για να δημιουργήσουμε το αρχείο κωδικού πρόσβασης πληκτρολογούμε την εντολή **htpasswd** την οποία μπορούμε αν βρούμε στο λογισμικό Apache . Το λογισμικό αυτό με την σειρά του θα αναζητήσει και θα βρει τον κατάλογο μέσα στον οποίον θα εγκατασταθεί το αρχείο κωδικού πρόσβασης , παραδείγματος χάριν , εάν ο Apache είναι εγκατεστημένος , μέσα στο σύστημα μας , ο κατάλογος στον οποίο θα αποθηκευτεί το αρχείο θα είναι ο ακόλουθος **/usr/local/apache/bin/htpasswd.**
Για αν δημιουργήσουμε τώρα κάποιο αρχείο πρόσβασης συγκεκριμένου τύπου θα πρέπει να πληκτρολογήσουμε : **htpasswd – όνομα χρήστη X / usr / local / apache /passwd / passwords.**
Αφού πληκτρολογήσουμε την εντολή αυτή , θα μας ζητηθεί στην συνέχεια να δακτυλογραφήσουμε τον κωδικό πρόσβασης που επιθυμούμε και στην συνέχεια να το επιβεβαιώσουμε πάλι .
Οι εντολές θα έχουν την ακόλουθη μορφή :
 # htpasswd – X / usr / local / apache passwd / passwords
Νέος κωδικός πρόσβασης : my password
Δακτυλογραφήστε εκ νέου τον κωδικό πρόσβασης : my password
Προστέθηκε ο κωδικός πρόσβασης στον χρήστη .

Με τις εντολές αυτές δημιουργείται ένα αρχείο πρόσβασης για τον χρήστη **X** και το οποίο τοποθετείται στην θέση ***/ usr / local / apache passwd / passwords***. Σε περίπτωση που θέλουμε να προσθέσουμε ένα ακόμη χρήστη στο αρχείο πρόσβασης αυτό , και αν το όνομα του νέου χρήστη είναι sugno , πληκτρολογούμε: **sugno */ usr / local / apache passwd / passwords*** . Στην περίπτωση αυτή θα ερωτηθούμε να παρέχουμε τον κωδικό πρόσβασης και να τον επιβεβαιώσουμε στην συνέχεια . Στις ίδιες ενέργειες θα πρέπει να προβούμε σε περίπτωση αντίστοιχη που θελήσουμε να αλλάξουμε το μονοπάτι στο οποίο αποθηκεύεται το αρχείο αυτό .

Ο κωδικός πρόσβασης αποθηκεύεται στο αρχείο κωδικού πρόσβασης με κρυπτογραφημένη μορφή , έτσι ώστε οι χρήστες του συστήματος να μην είναι σε θέση να διαβάσουν το αρχείο και να καθορίσουν αμέσως τους κωδικούς πρόσβασης όλων των χρηστών .

7.4.7.1.3 Πως διαμορφώνουμε τον τύπο Επικύρωσης του αρχείου κωδικού πρόσβασης .

Μόλις δημιουργήσουμε το αρχείο κωδικού πρόσβασης , πρέπει να οριοθετήσουμε στον Apache ποίος είναι ο σκοπός και ο λόγος δημιουργίας του συγκεκριμένου αρχείου , γιατί ενέργειες θα

χρησιμοποιηθεί κ.α. . Ο λόγος για τον οποίον πρέπει να γίνουν οι προσδιορισμοί αυτοί είναι για να απαιτηθούν και τα κατάλληλα πιστοποιητικά χρηστών για την αποδοχή . Αυτή η διαμόρφωση γίνεται με τις ακόλουθες οδηγίες :

AuthType: Καθορίζεται ο τύπος επικύρωσης που θα χρησιμοποιηθεί. Σε αυτήν την περίπτωση θα τεθεί ο τύπος Βασικός.

AuthName: Καθορίζεται η σφαίρα ή το όνομα της επικύρωσης.

AuthUserFile: Καθορίζεται η θέση του αρχείου του κωδικού πρόσβασης.

AuthGroupFile: Καθορίζεται η θέση του αρχείου ομάδας.

Απαιτήστε: Καθορίζεται τι κανόνες θα πρέπει να ικανοποιούνται προκειμένου να χορηγηθεί η άδεια πρόσβασης .

Αυτού του είδους οι οδηγίες τοποθετούνται μέσα στο αρχείο **X.htaccess** , αρχείο το οποίο περιέχεται σε έναν ιδιαίτερο φάκελο ο οποίος προστατεύεται ή μπορούν ακόμη να τοποθετηθούν στο κύριο αρχείο διαμόρφωσης που βρίσκεται στον κεντρικό υπολογιστή .
Ένα τέτοιο παράδειγμα , ενός ονόματος επικύρωσης το οποίο καλείται ¨από την αίτηση μόνο ¨, φαίνεται στις ακόλουθες εντολές .Το αρχείο του κωδικού πρόσβασης που βρίσκεται ***/ usr / local / apache passwd / passwords*** θα χρησιμοποιηθεί για να ελέγξει την ταυτότητα του χρήστη . Μόνο οι χρήστες που ονομάζονται sungo (ο κανόνας που θα πρέπει να ικανοποιείται στην απαίτηση) , θα χορηγούνται την πρόσβαση , και ακόμη και σε αυτήν την περίπτωση πάλι θα πρέπει να χορηγείτε και ο σωστός κωδικός πρόσβασης , ο οποίος θα πρέπει να είναι ίδιος με τον κωδικό πρόσβασης που είναι αποθηκευμένος στο αρχείο κωδικού πρόσβασης .

AuthType Βασικό.
AuthName "από την αίτηση μόνο".
AuthUserFile / usr / local / apache passwd / passwords.
Απαιτήστε ότι ο χρήστης θα ονομάζεται sungo

Την επόμενη φορά που θα φορτώσουμε κάποιο αρχείο από εκείνον τον κατάλογο , θα απαιτηθεί να δακτυλογραφήσουμε μόνο τον κωδικό πρόσβασης και το όνομα χρήστη προκειμένου να προχωρήσουμε .
Σημειώνουμε εδώ ότι μπορούμε ακόμη να προσδιορίσουμε τους χρήστες στους οποίου επιθυμούμε να παρέχεται άμεση άδεια πρόσβασης , διευκρινίζοντας ότι οποιοσδήποτε έγκυρος χρήστης θα έχει πρόσβαση άμεσα. Αυτό επιτυγχάνεται με την λέξη κλειδί ***έγκυρος –χρήστης.***
Στην τελευταία εντολή, στο απαιτήστε , έχει οριοθετηθεί η εντολή **Απαιτήστε τον έγκυρο – χρήστη** .

7.4.7.1.4 Πως δημιουργούμε ένα αρχείο ομάδας .

Η δημιουργία του αρχείου ομάδας είναι προαιρετική . Τις περισσότερες φορές θα θελήσουμε οι χρήστες μας να είναι περισσότεροι του ενός , ή δύο ή καμιά δωδεκαριά και όλοι θα θέλουν να έχουν πρόσβαση σε κάποιο πόρο . Θα θέλουμε σαν προγραμματιστές να είμαστε σε θέση να καθορίσουμε μια ομάδα ανθρώπων που να έχουν πρόσβαση σε έναν συγκεκριμένο πόρο , και να είμαστε σε θέση να διαχειριζόμαστε την ομάδα αυτή , να μπορούμε δηλαδή να προσθέτουμε ή να διαγράφουμε μέλη , χωρίς να πρέπει να εκδίδεται κάθε φορά το αρχείο διαμόρφωσης των κεντρικών υπολογιστών , και να ξεκινάει από την αρχή κάθε φορά ο Apache .

Αυτό το πρόβλημα αντιμετωπίζεται χρησιμοποιώντας τις ομάδες επικύρωσης . Μια ομάδα επικύρωσης , είναι όπως αναφέρεται και από το όνομα της , είναι ένας κατάλογος από μέλη .Αυτός ο κατάλογος αποθηκεύεται σε ένα αρχείο ομάδας το οποίο αποθηκεύεται στην ίδια θέση με το αρχείο κωδικού πρόσβασης , έτσι ώστε να είμαστε σε θέση να το ελέγχουμε άμεσα.
Η σύνταξη του αρχείου ομάδας είναι υπερβολικά απλή . Ένα όνομα ομάδας εμφανίζεται πρώτο σε μια γραμμή , το οποίο ακολουθείται από μια άνω και κάτω τελεία, και έπειτα ακολουθεί ένας κατάλογος των μελών της ομάδας τα οποία χωρίζονται σε διαστήματα . Παραδείγματος χάριν :
Συντάκτες(όνομα ομάδας): Anna , Daniel ,Allan .
Μόλις δημιουργήσουμε το αρχείο αυτό , μπορούμε να δηλώσουμε ότι κάποιο άτομο είναι μέλος της ομάδας αυτής , παίρνοντας τις ιδιότητες της , και αποκτώντας την πρόσβαση σε συγκεκριμένους πόρους . Αυτό γίνεται με τις παρακάτω εντολές ,και με την χρήση ενός AuthGroupFile.

AuthType Βασικό.
AuthName "συντάκτες".
AuthUserFile / usr / local / apache passwd / passwords
AuthUserFile / usr / local / apache passwd / groups
Απαιτήστε τους συντάκτες της ομάδας.

Η διαδικασία της επικύρωσης σε αυτό το σημείο είναι κάτι το απλό , αφού έχει ολοκληρωθεί η δημιουργία του αρχείου ομάδας , το οποίο και απλουστεύει τις ενέργειες που απαιτούνται από μεριά του χρήστη . Όταν εμφανιστεί κάποιο αίτημα επικύρωσης ,και αφού προσκομίσουν το όνομα χρήστη και ο κωδικός πρόσβασης , αυτό που αναζητείται είναι το αρχείο ομάδας , μέσω του αρχείου αυτού ελέγχεται εάν το όνομα χρήστη ανήκουν στην απαραίτητη ομάδα χρηστών . Εάν αυτό συμβαίνει στην συνέχεια και μέσω πάλι του αρχείου ομάδας ελέγχεται ο κωδικός πρόσβασης και εάν για το συγκεκριμένο όνομα χρήστη που ανήκει στην ομάδα αυτή, αντιστοιχεί ο κωδικός αυτός . Σε περίπτωση που όλα τα βήματα που προαναφέραμε ολοκληρωθούν ορθά , παρέχεται η πρόσβαση στον χρήστη , εάν κάποιο από τα βήματα αυτά αποτύχει να ολοκληρωθεί , η πρόσβαση απαγορεύεται για τον συγκεκριμένο χρήστη .

7.4.7.1.5 Ελαττώματα της βασικής επικύρωσης

Η βασική επικύρωση , είναι μια από τις πιο ευρέως χρησιμοποιημένες μεθόδους επικύρωσης ,δεν παύει όμως να διαθέτει και κάποια αδύνατα σημεία τα οποία θα πρέπει να αναφερθούν για την καλύτερη ενημέρωση των χρηστών . Αρχικά θα πρέπει να γίνει γνωστό ότι η βασική επικύρωση δεν πρέπει να χρησιμοποιείται σε περιπτώσεις που επιθυμούμε ιδιαίτερα αυστηρή ασφάλεια.
Αν και ο κωδικός πρόσβασης αποθηκεύεται στον κεντρικό υπολογιστή, κρυπτογραφημένος ,πράγμα που τον καθιστά ασφαλή απέναντι στους κακόβουλους χρήστες , η προσπέλασή του κωδικού αυτού από τον χρήστη προς τον κεντρικό υπολογιστή , γίνεται μέσω του δικτύου . Το γεγονός αυτό αποτελεί τρωτό σημείο της βασικής επικύρωσης , για τον λόγο ότι εάν κάποιος κακόβουλος χρήστης παρακολουθεί και ¨ακούει ¨ τα πακέτα που μεταφέρουμε μπορεί να είναι σε θέση να διαβάσει και να υποκλέψει το όνομα χρήστη και τον κωδικό πρόσβασης καθώς αυτά μεταφέρονται .
Δεύτερο τρωτό σημείο της βασικής επικύρωσης αποτελεί το γεγονός ότι αν θυμηθούμε την διαδικασία της λειτουργίας της μεθόδου αυτή όπως την αναλύσαμε προηγουμένως θα δούμε ότι το όνομα χρήστη και ο κωδικός πρόσβασης μεταφέρονται με κάθε αίτημα , όχι μόνο όταν δακτυλογραφηθούν από τον χρήστη αλλά και από μόνα τους . Λόγω λοιπόν αυτού εάν ο

κακόβουλος χρήστης παρακολουθεί τις αιτήσεις μας για αρκετό χρονικό διάστημα , μπορεί να είναι σε θέση να υποκλέψει στα σημαντικά αυτά στοιχεία μας .
Για τους λόγους , λοιπόν αυτούς καλό θα ήταν να μην χρησιμοποιούμε την βασική επικύρωση σε περιπτώσεις που επιθυμούμε πραγματική ασφάλεια . Γιατί μπορεί να προκληθούν ανεπανόρθωτες βλάβες στα συστήματα μας και οι πληροφορίες μας να δεχτούν σημαντική εκμετάλλευση , καθώς οι χρήστες εκείνοι που θα προσπαθήσουν να ενισχύσουν τις αδυναμίες αυτές μέσω ειδικού λογισμικού και εξοπλισμού , θα είναι λίγοι .
Εντούτοις η βασική επικύρωση μέσω μιας SSL σύνδεσης , είναι περισσότερο ασφαλής καθώς όλα τα δεδομένα και ο κωδικός πρόσβασης με το όνομα χρήστη , είναι κρυπτογραφημένα .

7.4.7.2 Επικύρωση Αφομοιώσεων .

Ο δεύτερος τύπος επικύρωσης που θα μελετήσουμε θα είναι αυτός των αφομοιώσεων .

7.4.7.2.1 Πως λειτουργεί η επικύρωση αφομοιώσεων .

Η επικύρωση αφομοιώσεων εφαρμόζεται μέσω νέων μηχανισμών οι οποίοι είναι συμβατοί με τις μηχανές αναζήτησης μας . Παρουσιάζουν έτσι μεγαλύτερες προδιαγραφές ασφάλειας . Χρησιμοποιώντας την επικύρωση αφομοιώσεων , η βασική διαφορά που παρατηρούμε και η οποία αξίζει να αναφερθεί είναι το γεγονός ότι , ο κωδικός πρόσβασης μας δεν στέλνεται ποτέ σαφής μέσα στο δίκτυο , αλλά διαβιβάζεται πάντα μέσω της χρήσης ενός MD5 πρωτοκόλλου το οποίο ¨αφομοιώνει ¨τον κωδικό πρόσβασης του χρήστη και μεταβιβάζει κωδικοποιημένες πληροφορίες . Με αυτόν τον τρόπο ο κωδικός πρόσβασης δεν μπορεί να υποκλαπεί από κακόβουλους χρήστες μέσω διαδικασιών όπως το ¨άκουσμα¨ της κυκλοφορίας του δικτύου .

7.4.7.2.2 Πως δημιουργούμε ένα αρχείο κωδικού πρόσβασης .

Η διαδικασία της δημιουργίας ενός αρχείου κωδικού πρόσβασης στην επικύρωση αφομοιώσεων , δεν παρουσιάζει σημαντικές αλλαγές από την αντίστοιχη διαδικασία η οποία συντελείται στην βασική επικύρωση .
Για οποιαδήποτε χρήση και αν θέλουμε να επικαλεστούμε τον μηχανισμό της επικύρωσης , έστω και για μια πολύ απλή λειτουργία , θα πρέπει να δημιουργήσουμε και να διατηρήσουμε ένα αρχείο κωδικού πρόσβασης το οποίο και θα ισχύει μεμονωμένα για κάθε χρήστη .
Στον Apache η λειτουργία αυτή της δημιουργίας του αρχείου κωδικού πρόσβασης ονομάζεται **htdigest** ,την οποία και μπορούμε να βρούμε κατάλογο εργασιών του Apache .
Για να δημιουργήσουμε τώρα ένα αρχείο κωδικού πρόσβασης τύπου αφομοιώσεων θα πρέπει να πληκτρολογήσουμε τις ακόλουθες εντολές:

 # htdigest- όνομα χρήστη X / usr / local / apache passwd / digest
Νέος κωδικός πρόσβασης : my password
Δακτυλογραφήστε εκ νέου τον κωδικό πρόσβασης : my password
Προστέθηκε ο κωδικός πρόσβασης στον χρήστη .

Στο σημείο αυτό θα μας ζητηθεί από την λειτουργιά htdigest , ο κωδικός πρόσβασης που επιθυμούμε να ορίσουμε , και αφού τον δακτυλογραφήσουμε , θα μας ζητηθεί να τον επιβεβαιώσουμε πάλι στην συνέχεια .
Και σε αυτόν τον τύπο επικύρωσης , όπως και στην βασική επικύρωση , μας συστήνεται να αποθηκεύουμε τις λεπτομέρειες αυτές σε μια τοποθεσίας έξω από τον κατάλογο των εγγραφών .
Επίσης ομοίως με την εντολή htpasswd –X η λειτουργία αυτή δημιουργεί ένα νέο αρχείο ή εάν υπάρχει το αρχείο με την ονομασία αυτή , διαγράφει το περιεχόμενο του αρχείου αυτού και εναποθέτει στο εσωτερικό του τα νέα δεδομένα

7.4.7.2.3 Πως διαμορφώνουμε τον τύπο Επικύρωσης του αρχείου κωδικού πρόσβασης .

Ομοίως και σε αυτόν τον τύπο της επικύρωσης , όταν δημιουργήσουμε το αρχείο του κωδικού πρόσβασης θα πρέπει να διευκρινίσουμε στον Apache , ποιος είναι ο κύριος λόγος δημιουργίας του αρχείου αυτού . Προκειμένου αυτός με την σειρά του να απαιτήσει από την πηγή προέλευσης τα απαραίτητα πιστοποιητικά επικύρωσης .
Η διαμόρφωση αυτή γίνεται ακολουθώντας τις παρακάτω οδηγίες :

AuthType: Καθορίζεται ο τύπος επικύρωσης που θα χρησιμοποιηθεί. Σε αυτήν την περίπτωση θα τεθεί ο τύπος Αφομοίωση.

AuthName: Καθορίζεται η σφαίρα ή το όνομα της επικύρωσης.

AuthDigestFile: Καθορίζεται η θέση του αρχείου του κωδικού πρόσβασης.

AuthDigestGroupFile: Καθορίζεται η θέση του αρχείου ομάδας.

Απαιτήστε: Καθορίζεται τι κανόνες θα πρέπει να ικανοποιούνται προκειμένου να χορηγηθεί η άδεια πρόσβασης .

Αυτού του είδους οι οδηγίες τοποθετούνται μέσα στο αρχείο **X.htaccess** , αρχείο το οποίο περιέχεται σε έναν ιδιαίτερο φάκελο ο οποίος προστατεύεται ή μπορούν ακόμη να τοποθετηθούν στο κύριο αρχείο διαμόρφωσης που βρίσκεται στον κεντρικό υπολογιστή .
Το ακόλουθο παράδειγμα καθορίζει ένα κύκλο επικύρωσης ο οποίος αποκαλείται ¨ιδιωτική¨ . Το αρχείο κωδικού πρόσβασης που βρίσκεται ***/ usr / local / apache passwd / digest*** θα χρησιμοποιηθεί για να ελέγξει την ταυτότητα του χρήστη . Μόνο οι χρήστες οι οποίοι θα φέρουν την ονομασία *drbacchus ή dorfl* θα τους χορηγείται πρόσβαση , και αυτοί πάλι με την προϋπόθεση ότι θα δακτυλογραφούν ορθά τον απαραίτητο κωδικό πρόσβασης .

AuthType Αφομοίωση.
AuthName “Ιδιωτική”.
AuthDigestFile / usr / local / apache/ passwd /digest

Απαιτήστε τους χρήστες drbacchus, dorfl

7.4.7.2.4 Πως δημιουργούμε ένα αρχείο ομάδας .

Όπως έχουμε παρατηρήσει μέχρι στιγμής δεν υπάρχουν σημαντικές διαφορές ανάμεσα στους δύο τύπους επικύρωσης . Και στο κομμάτι της δημιουργίας ενός αρχείου ομάδας οι ομοιότητες είναι εμφανής . Το αρχείο ομάδας που χρησιμοποιούμε για την επικύρωση αφομοιώσεων είναι ακριβώς το ίδιο με αυτό που χρησιμοποιείται για την βασική επικύρωση . Δηλαδή οι εντολές που αποτελούν το αρχείο ομάδας είναι , το όνομα της ομάδας , μια άνω και κάτω τελεία και ο κατάλογος των μελών της ομάδας αυτής . Παραδείγματος χάριν :
Admins: Jim, Anna, Mary
Μόλις δημιουργήσουμε το αρχείο αυτό , είμαστε σε θέση να ορίσουμε το ποιός χρήστης θα είναι μέλος της ομάδας αυτής, και ως αποτέλεσμα θα του χορηγείτε πρόσβαση στον πόρο . Η χορήγηση της εισόδου πρόσβασης σε ένα πόρο γίνεται με την εντολή **AuthDigestGroupFile** όπως φαίνεται και στο παρακάτω παράδειγμα .
AuthType Αφομοίωση.
AuthName "ιδιωτικό".
AuthUserFile / usr / local / apache passwd / passwords
AuthUserFile / usr / local / apache passwd / groups
Απαιτήστε τους συντάκτες της ομάδας.

Όπως παρατηρούμε , η διαδικασία της επικύρωσης είναι ίδια με αυτή του βασικού τύπου . Αρχικά ελέγχεται ο χρήστης , το αν βρίσκεται δηλαδή στην σωστή ομάδα , και εάν αυτό ισχύει στην συνέχεια ελέγχεται ο κωδικός πρόσβασης.

7.4.7.2.5 Ελαττώματα της επικύρωσης αφομοιώσεων .

Όπως σχεδόν όλοι οι μηχανισμοί επικύρωσης , έτσι και η επικύρωση αφομοιώσεων παρουσιάζει κάποια προτερήματα αλλά και ελαττώματα . Αρχικά θα αναφέρουμε το μεγάλο πλεονέκτημα που διαθέτει αυτός ο τύπος της επικύρωσης , το οποίο και είναι ότι δεν αποστέλλει αποσαφηνισμένο τον κωδικό πρόσβασης μέσω του δικτύου . Η λειτουργία αυτή βέβαια δεν υποστηρίζεται από όλες της σημαντικές μηχανές αναζήτησης , και για αυτόν τον λόγο δεν θα πρέπει να την χρησιμοποιούμε σε Ιστοχώρους που δεν μπορούμε να ελέγξουμε τις μηχανές αναζήτησης που οι χρήστες πρόκειται να χρησιμοποιήσουν .
Όσον αφορά τώρα τα επίπεδα ασφάλειας , πρέπει να καταλάβουμε δύο πράγματα . Βασικά αν και ο κωδικός πρόσβασης μας δεν περνάει αποσαφηνισμένος μέσα στο δίκτυο , δεν γίνεται το ίδιο για όλα τα υπόλοιπα προσωπικά μας δεδομένα . Γεγονός που αξιολογείται ως ελλιπές μέτρο ασφάλειας αυτού του τύπου επικύρωσης . Δεύτερον αν και ο κωδικός πρόσβασης μας στην πραγματικότητα δεν αποστέλλεται , στην πραγματικότητα αποστέλλεται μια μορφή αφομοιώσεως αυτού , κάποιος πολύ έμπειρος χρήστης , ο οποίος είναι εξοικειωμένος με την λειτουργία του HTTP , μπορεί να είναι σε θέση να χρησιμοποιήσει αυτές τις πληροφορίες μας και να ανακτήσει τον κωδικό πρόσβασης μας , αποκτώντας έτσι πρόσβαση στις πληροφορίες . Δεδομένου ότι ο αφομοιωμένος κωδικός πρόσβασης μας περιέχει όλες τις πληροφορίες που απαιτούνται για να έχουμε πρόσβαση , σε κάποιον πόρο ή στον Ιστοχώρο .
Για την αντιμετώπιση του μειονεκτήματος αυτού , προτείνεται η χρήση SSL πρωτοκόλλου , με σκοπό να διατηρηθούν τα περιεχόμενα μας ασφαλή .

7.4.7.3 Μηχανισμός Ελέγχου Πρόσβασης .

Η επικύρωση ενός χρήστη βασισμένη στο όνομα χρήστη ή στον κωδικό πρόσβασης , είναι ένα κομμάτι των όλων διαδικασιών . Συχνά σαν χρηστές διαχειριστές επιθυμούμε να επιτρέψουμε την είσοδο σε άλλους χρήστες με βάση κάποιο άλλο στοιχείο εκτός του γεγονότος το ποιοι είναι . Βάση λοιπόν αυτής της επιθυμίας μας προκύπτει ο μηχανισμός Ελέγχου πρόσβασης .

7.4.7.3.1 Αποδοχή ή Απόρριψη

Οι εντολές αποδοχή ή απόρριψη χρησιμοποιούνται για να επιτρέψουμε ή να αρνηθούμε την πρόσβαση σε κάποιον χρήστη με βάση κάποια χαρακτηριστικά στοιχεία . Η αποδοχή ή η απόρριψη αυτή μπορεί να βασίζεται είτε στον host name , είτε στο host address, και επιτυγχάνεται με την ζήτηση ενός εγγράφου από την μηχανή αναζήτησης που χρησιμοποιεί ο εκάστοτε χρήστης .
Οι εντολές αυτές ονομάζονται αλλιώς και ως Διαταγές (όπως αναφέρονται στον apache), οι οποίες εντολές ¨διατάζουν ¨ τις μηχανές αναζήτησης των χρηστών να εφαρμόσουν τα φίλτρα του είδους που εμείς επιθυμούμε .
Η σύνταξη αυτών των εντολών έχει την ακόλουθη μορφή :
Επιτρέψτε από την διεύθυνση
όπου η διεύθυνση είναι μια IP διεύθυνση ή κάποιο όνομα περιοχών , μπορούμε να επιδιώκουμε να επιτρέπονται ή να απορρίπτονται πολλαπλά ονόματα διευθύνσεων ή περιοχών .

Για παράδειγμα εάν έχουμε κάποιαν διεύθυνση που επιθυμούμε να μην περιλαμβάνεται σε κάποιο πίνακα μηνυμάτων μας , μπορούμε να πληκτρολογήσουμε το εξής :
Απορρίψτε από το 11.22.33.44
Οι επισκέπτες που προέρχονται από εκείνην την διεύθυνση δεν θα είναι σε θέση να έχουν πρόσβαση σε κάποια περιεχόμενα , λόγω αυτής της εντολής . Εάν σε αντίθεση διαθέτουμε κάποιο όνομα μηχανών , αντί της διεύθυνσης που διαθέταμε πριν , μπορούμε να χρησιμοποιήσουμε την ακόλουθη εντολή :
Απορρίψτε από το hostname.example.com

Παρόμοιες εντολές χρησιμοποιούμε εάν επιθυμούμε να εμποδίσουμε την πρόσβαση σε μια ολόκληρη περιοχή ή σε ένα ολόκληρο tld (κορυφαία περιοχή , όπως για παράδειγμα το .com ή το .gov) .Μπορούμε και σε αυτήν την περίπτωση να διευκρινίσουμε μέρος του ονόματος διευθύνσεων ή των περιοχών που επιθυμούμε να απορρίψουμε :
Απορρίψτε από 192.101.205
Απορρίψτε από το exampleone.com , exampletwo.com
Απορρίψτε από το tld

7.4.7.4 Επικύρωση διαδικτύου , Πρωτόκολλα επικύρωσης .

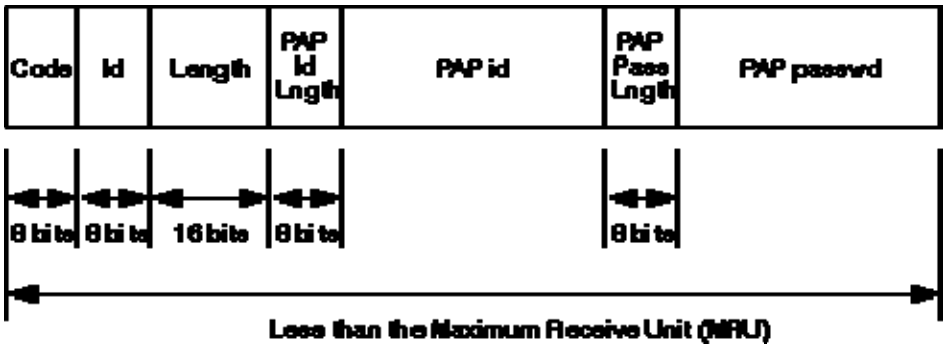
7.4.7.4.1 Password Authentication Protocol(PAP).

Το Password Authentication Protocol (PAP) είναι ένα απλό πρωτόκολλο επικύρωσης που χρησιμοποιείται για την επικύρωση ενός χρήστη σε κάποιο Διακομιστή Πρόσβασης Δικτύου (Network Access Server, NAS) που μπορεί να χρησιμοποιείται για παράδειγμα από παρόχους υπηρεσιών Ίντερνετ . Το PAP χρησιμοποιείται από πρωτόκολλο PPP . Το PAP μεταδίδει μη κρυπτογραφημένους ASCII κωδικούς μέσω δικτύου και για αυτόν τον λόγο θεωρείται μη ασφαλές πρωτόκολλο.
Χρησιμοποιείται ως έσχατη λύση όταν ο απομακρυσμένος διακομιστής δεν υποστηρίζει πιο ισχυρό πρωτόκολλο επικύρωσης , όπως το CHAP ή το EAP .

Βήματα εργασίας πρωτοκόλλου.

1. Ο πελάτης αποστέλλει όνομα χρήστη και κωδικό πρόσβασης .
2. Ο διακομιστής αποστέλλει μήνυμα authentication-ack εάν τα διαπιστευτήρια είναι αποδεκτά ή εναλλακτικά authentication-nak εάν δεν είναι αποδεκτά .

Στο σχήμα που ακολουθεί παρουσιάζεται η δόμηση ενός PAP πακέτου , το οποίο ενθυλακώνεται μέσα σε ένα PPP Frame .



Εικόνα 100 :Δομή ενός PAP πακέτου .

7.4.7.4.2 Extensible Authentication Protocol(EAP).

Το πρωτόκολλο Extensible Authentication Protocol ή αλλιώς EAP είναι ένα παγκόσμιο πλαίσιο επικύρωσης που χρησιμοποιείται συχνά στα ασύρματα δίκτυα και στις Point-to-Point συνδέσεις .
Αν και η λειτουργία του πρωτοκόλλου EAP δεν περιορίζεται μόνο σε ασύρματα δίκτυα LAN και μπορεί να χρησιμοποιηθεί και σε ενσύρματες συνδέσεις , παρόλα αυτά συχνότερα εμφανίζεται

σε ασύρματα δίκτυα . Προσφάτως τα πρότυπα WPA και WPA2 έχουν υιοθετήσει επίσημα πέντε τύπους των EAP πρωτοκόλλων ως επίσημους μηχανισμούς επικύρωσης .
Το EAP είναι ένα πλαίσιο επικύρωσης και όχι ένας συγκεκριμένος μηχανισμός , παρέχει μερικές κοινές λειτουργίες και μια διαπραγμάτευση του επιθυμητού μηχανισμού επικύρωσης . Τέτοιου είδους μηχανισμοί καλούνται μέθοδοι EAP , αυτήν την περίοδο υπάρχουν περίπου 40 τέτοιοι μηχανισμοί . Οι μέθοδοι που καθορίζονται από IETF RFCs περιλαμβάνουν EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS,EAP-IKEv2, EAP-SIM, και EAP-AKA .
Οι πιο χρησιμοποιημένες σύγχρονες μέθοδοι οι οποίες και είναι πολύ ικανές για την χρήση τους στα ασύρματα δίκτυα περιλαμβάνουν EAP-SIM , EAP-AKA και EAP-TLS .
Όταν μια EAP μέθοδος επικαλείται από μια 802.1X NAS (κεντρικός υπολογιστής πρόσβασης στο δίκτυο) συσκευή όπως ένα ασύρματο σημείο πρόσβασης 802.11 a/b/g , οι σύγχρονες αυτές μέθοδοι παρέχουν έναν ασφαλή μηχανισμό επικύρωσης και διαπραγματεύονται ένα ασφαλές PMK (Pair-wise Master Key) μεταξύ του πελάτη και του NAS . Το PMK μπορεί στην συνέχεια να χρησιμοποιηθεί για την ασύρματη σύνοδο κρυπτογράφησης που χρησιμοποιεί (βασισμένο σε AES) την κρυπτογράφηση TKIP ή CCMP .
Το EAP δεν είναι ένα ασύρματο πρωτόκολλο , αντ αυτού καθορίζει μόνο το σχήμα των μηνυμάτων . Κάθε πρωτόκολλο το οποίο χρησιμοποιεί EAP καθορίζει ένα τρόπο ενθυλάκωσης EAP μηνυμάτων μέσα στα μηνύματα του πρωτοκόλλου εκείνου. Στην περίπτωση 802.1X , αυτή η ενθυλάκωση ονομάζεται EAPOL(EAP over LANs).
Στην συνέχεια θα ακολουθήσει μια περιγραφή και των υπόλοιπων συσχετιζόμενων πρωτοκόλλων επικύρωσης . Μερικά παραδείγματα αυτών είναι τα LEAP,EAP-TLS , EAP-MD5, EAP-PSK, EAP-TTLS,EAP-IKEv2, PEAP ,EAP-FAST, EAP-AKA κα.

LEAP

Το Lightweight Extensible Authentication Protocol (LEAP) είναι μια ιδιόκτητη μέθοδος EAP που δημιουργήθηκε από την Cisco Systems πριν από την IEEE επικύρωση προτύπων ασφάλειας 802.1.1i. Η εταιρία Cisco διανέμει το πρωτόκολλο μέσω του CCX(Cisco Certified eXtensions) ως τμήμα του 802.1X και υιοθετεί την δυναμική του WEP προτύπου .
Τα LEAP χρησιμοποιούν μια τροποποιημένη έκδοση του MS-CHAP , μια επικύρωση πρωτοκόλλων στην οποία τα πιστοποιητικά του χρήστη δεν είναι ισχυρά προστατευμένα και μπορούν εύκολα να συμβιβαστούν .
Για τον λόγο αυτό η Cisco , συστήνει στους πελάτες της που χρησιμοποιούν αποκλειστικά LEAP ,να το κάνουν μόνο με την χρήση αρκετά σύνθετων κωδικών πρόσβασης , αν και οι οποίοι μπορεί να είναι πολύ δύσκολο να διαχειριστούν από αυτούς.
Η Cisco γενικά προτείνει να χρησιμοποιούμε τα νεώτερα και περισσότερο ισχυρά πρωτόκολλα EAP – FAST, PEAP , EAP-TLS.

EAP-TLS

Το EAP-Transport Layer Security ή αλλιώς EAP-TLS όπως ονομάζεται, είναι ένα IETF ανοικτό πρότυπο , και υποστηρίζεται αρκετά από τους προμηθευτές των ασύρματων δικτύων . Η ασφάλεια του TLS (επίσημα στο παρελθόν , όπως ανεπίσημα και στο παρόν εμφανίζεται συχνά να αναφέρεται Secure Sockets Layer), πρωτοκόλλου είναι αρκετά ισχυρή , αρκεί βεβαίως οι χρήστες να καταλαβαίνουν τις προειδοποιήσεις και να προλαμβάνουν τα πιθανά ψεύτικα πιστοποιητικά .
Το πρωτόκολλο αυτό χρησιμοποιεί PKI για να ασφαλίσει την επικοινωνία στον κεντρικό υπολογιστή RADIUS επικύρωσης ή σε κάποιον άλλο τύπο επικύρωσης κεντρικού υπολογιστή . Έτσι ακόμη και αν το πρωτόκολλο EAP-TLS παρέχει άριστη ασφάλεια , τα μεγάλα πιστοποιητικά από μεριάς πελάτη ίσως αποτελούν την αχίλλειον φτέρνα του .
Το EAP-TLS είναι το αυθεντικό πρότυπο ασύρματου LAN EAP πρωτόκολλου επικύρωσης . Αν και η επέκταση του είναι ένα γεγονός σπάνιο , θεωρείται ένα από τα ασφαλέστερα διαθέσιμα

πρότυπα EAP και υποστηρίζεται παγκοσμίως από όλους τους κατασκευαστές του ασύρματου υλικού και του λογισμικού του τοπικού δικτύου συμπεριλαμβανομένης και της Microsoft .
Η απαίτηση από μεριάς πελάτη ενός πιστοποιητικού , όσο μη δημοφιλής και να είναι , δίνει στο EAP –TLS πρωτόκολλο δυνατή επικύρωση και επεξηγεί την κλασσική ευκολία σε αντίθεση με την ασφάλεια ανταλλαγής .
Ένας συμβιβασμένος κωδικός πρόσβασης δεν είναι αρκετός να ¨σπάσει ¨ μέσα στα πρωτόκολλα EAP-TLS επειδή ο χάκερ θα πρέπει ακόμη να διαθέτει το δευτερεύον ιδιωτικό κλειδί του πελάτη . Ακόμη υψηλότερα επίπεδα ασφάλειας επιτυγχάνονται μέσω της χρήσης των έξυπνων καρτών .
Αυτό συμβαίνει επειδή δεν υπάρχει κανένας τρόπος να κλαπεί το ιδιωτικό κλειδί ενός πιστοποιητικού από μια έξυπνη κάρτα , χωρίς να έχει προηγηθεί κλοπή της ίδιας της κάρτας . Είναι όμως φυσικό επακόλουθο ότι η κλοπή της ίδιας της κάρτας θα γίνει αντιληπτή από τον , με αποτέλεσμα ο ιδιοκτήτης της κάρτας να έχει την δυνατότητα να σφραγίσει άμεσα την έξυπνη κάρτα αχρηστεύοντας έτσι τον κωδικό πρόσβασης που αυτή μεταφέρει.
Τέλος υπάρχουν πολλές εφαρμογές κεντρικών υπολογιστών και υπολογιστών πελατών οι οποίες υποστηρίζουν τα EAP-TLS πρωτόκολλα . Τα πρωτόκολλα αυτά υποστηρίζονται ακόμη από λειτουργικά συστήματα όπως το Mac OS X 10.3 τα Windows 2000 SP4 , Windows XP, Windows Vista , Windows Server 2003, Windows Mobile 2003 και τα Windows CE 4.2.

EAP-MD5

Το επόμενο πρωτόκολλο στο οποίο θα αναφερθούμε είναι το EAP-MD5, και είναι το μοναδικό πρότυπό IETF πρωτοκόλλων που βασίζεται στην μέθοδο διαδρομής EAP. Προσφέρει σχετικά μικρή ασφάλεια , καθώς η MD5 hash λειτουργία είναι σχετικά τρωτή σε επιθέσεις λεξικών , και δεν υποστηρίζει την παραγωγή κλειδιού , η οποία καθίσταται ακατάλληλη για την χρήση dynamic WEP ή WPA/WPA2 σε επιχειρήσεις . Το EAP-MD5 πρωτόκολλο διαφέρει από τις μεθόδους των άλλων EAP πρωτοκόλλων δεδομένου ότι παρέχει την επικύρωση του EAP Peep το στον κεντρικό υπολογιστή , αλλά όχι την αμοιβαία επικύρωση . Με το να μην παρέχει την επικύρωση κεντρικών υπολογιστών EAP , η μέθοδος αυτή καθίσταται τρωτή σε ατομικές μέσες επιθέσεις .

EAP-PSK

Το πρωτόκολλο EAP-PSK είναι μια μέθοδος EAP για την αμοιβαία επικύρωση και την βασική παραγωγή συνόδου που χρησιμοποιεί ένα προ-κοινό κλειδί (PSK). Παρέχει ένα προστατευμένο κανάλι επικοινωνίας όταν η αμοιβαία επικύρωση είναι επιτυχής για αμφότερα τα συμβαλλόμενα μέρη και σχεδιάστηκε για την επικύρωση πέρα από τα επισφαλή δίκτυα όπως το IEEE 802.11.
Το πρωτόκολλο EAP-PSK είναι τεκμηριωμένο σε ένα πειραματικό RFC το οποίο παρέχει μια ελαφριά και επεκτάσιμη μέθοδος EAP , η οποία δεν απαιτεί ένα κρυπτογραφημένο δημόσιο κλειδί . Η μέθοδος ανταλλαγή πρωτοκόλλων EAP ολοκληρώνεται με την χρήση το πολύ τεσσάρων μηνυμάτων .

EAP-TTLS

Το πρωτόκολλο EAP-Tunneled Transport Layer Security ή αλλιώς EAP-TTLS , είναι ένα πρωτόκολλο EAP το οποίο επεκτείνει το TLS πρωτόκολλο . Συντάχτηκε από την εταιρεία Funk Software and Certicom , και υποστηρίζεται ευρέως στις πλατφόρμες , ένα και δεν υπάρχει καμία εγγενής υποστήριξη OS για αυτό το EAP πρωτόκολλο στα Windows της Microsoft, γεγονός που απαιτεί την εγκατάσταση μικρών πρόσθετων προγραμμάτων όπως για παράδειγμα του SecureW2.
Το πρωτόκολλο EAP-TTLS προσφέρει πολύ καλού επιπέδου ασφάλεια . Ο πελάτης δεν χρειάζεται να επικυρωθεί μέσω CA-υπογεγραμμένου πιστοποιητικού στον server , αλλά μόνο στον κεντρικό υπολογιστή του πελάτη . Αυτό απλοποιεί πολύ την διαδικασία οργάνωσης δεδομένου ότι ένα πιστοποιητικό δεν πρέπει να εγκαθίσταται σε κάθε πελάτη .

Αφότου επικυρώνεται ασφαλώς ο κεντρικός υπολογιστής του πελάτη μέσω του CA – πιστοποιητικού , ο κεντρικός υπολογιστής μπορεί έπειτα να χρησιμοποιήσει την καθιερωμένη ασφαλή σύνδεση ¨τούνελ ¨ για να επικυρώσει τον πελάτη . Μπορεί ακόμη να χρησιμοποιήσει μια υπαρκτή και ευρέως επεκτεινόμενης επικύρωση πρωτοκόλλου , και υποδομή ενσωματώνοντας τους μηχανισμούς κωδικού πρόσβασης κληρονομιών και τις βάσεις δεδομένων επικύρωσης , ενώ η ασφαλής σήραγγα παρέχει την προστασία από επιθέσεις τύπου ¨κρυφακούσματος ¨ και αυτές του κατά ατόμου μεσαίων επιθέσεων .
Σημειώνουμε ακόμη ότι το όνομα του χρήστη δεν διαβιβάζεται ποτέ μέσα στο δίκτυο μη κρυπτογραφημένο . βελτιώνοντας κατά συνέπεια την μυστικότητα των πελατών .

EAP-IKEv2
Το πρωτόκολλο EAP-IKEv2 είναι μια EAP μέθοδος η οποία βασίζεται στα πρωτόκολλα ανταλλαγής κλειδιών Ιντερνετ έκδοσης 2 (Internet Key Exchange Protocol Version 2-IKEv2). Τα πρωτόκολλα αυτά παρέχουν επικύρωση και βασική καθιέρωση συνόδων μεταξύ ενός EAP peer και ενός EAP server . Ακόμη υποστηρίζει τεχνικές επικύρωσης οι οποίες είναι βασισμένες στους ακόλουθους τύπους πιστοποιητικών :

- Ασυμμετρικά ζευγάρια κλειδιών – δημόσια/ιδιωτικά ζευγάρια κλειδιών , όπου το δημόσιο κλειδί ενσωματώνεται μέσα σε ένα ψηφιακό πιστοποιητικό , και το αντίστοιχο ιδιωτικό είναι γνωστό μόνο σε ένα ενιαίο συμβαλλόμενο μέρος .
- Κωδικοί πρόσβασης – σειρές strings χαμηλής εντροπίας , που είναι γνωστά ταυτόχρονα και στον server αλλά και στον peer .
- Συμμετρικά κλειδιά –σειρές strings υψηλής εντροπίας , που είναι γνωστά ταυτόχρονα και στον server αλλά και στον peer .

Είναι πιθανόν ακόμη , να χρησιμοποιηθεί ένα διαφορετικό πιστοποιητικό επικύρωσης (και με αυτόν τον τρόπο τεχνικής) για κάθε κατεύθυνση . Παραδείγματος χάριν , ο EAP server επικυρώνεται χρησιμοποιώντας το δημόσιο /ιδιωτικό ζευγάρι κλειδιών και ο EAP peer χρησιμοποιώντας το συμμετρικό κλειδί EAP . Στην εικόνα που ακολουθεί παρουσιάζονται κάποιοι ιδιαίτεροι συνδυασμοί που αναμένεται να χρησιμοποιηθούν στην πράξη :

Πίνακας 9: Συνδυασμοί τύπων πιστοποιητικών .

EAP server	EAP peer
Asymmetric key pair	Asymmetric key pair
Asymmetric key pair	Symmetric key
Asymmetric key pair	Password
Symmetric key	Symmetric key

PEAP

Το Protected Extensible Authentication Protocol – Protected EAP ή αλλιώς απλά PEAP , είναι ένα πρωτόκολλο με το οποίο μεταφέρουμε με ασφαλή τρόπο , πληροφορίες συμπεριλαμβανομένων των κωδικών πρόσβασης, σε ένα ενσύρματο ή ασύρματο δίκτυο . Αναπτύχθηκε από κοινού από τις εταιρείες Cisco Systems , Microsoft και RSA Security . Σημειώνουμε ακόμη ότι το PEAP είναι ένα μη κρυπτογραφημένο πρωτόκολλο , όπως και τα υπόλοιπα EAP πρωτόκολλα , τα οποία χρησιμοποιούνται μόνο για την επικύρωση ενός πελάτη μέσα σε ένα δίκτυο .
Τα PEAP χρησιμοποιούν από την πλευρά του server πιστοποιητικά δημοσίου κλειδιού για να επικυρώσουν τον server . Στην συνέχεια δημιουργούν ένα κρυπτογραφημένο SSL/TLS πέρασμα μεταξύ του πελάτη και του επικυρωμένου server . Η επόμενη ανταλλαγή πληροφοριών επικύρωσης που αποστέλλονται με σκοπό να επικυρώσουν κρυπτογραφούνται , με αυτόν τον τρόπο τα πιστοποιητικά του χρήστη είναι ασφαλή από το να τα υποκλέψει κάποιο κρυφακούγοντάς τα .
Τα PEAP είναι κοινή πρόταση των εταιρειών Cisco Systems , Microsoft και της RSA Security . Είναι ήδη ευρέως διαθέσιμα σε πολλά προϊόντα και παρέχουν πολύ καλή ασφάλεια . Στον σχεδιασμό είναι παρόμοια με τα EAP-TTLS , απαιτώντας μόνο από την μεριά του server PKI πιστοποιητικά προκειμένου να δημιουργήσουν μια ασφαλή TLS διαδρομή μετάδοσης προστατεύοντας έτσι την επικύρωση του χρήστη .
Από τον Μάιο του 2005 και μετά είναι διαθέσιμες δύο υποκατηγορίες που πιστοποιούνται για τα ενημερωμένα WPA και WPA2 πρότυπα .

- Το PEAPv0/EAP-MSCHAPv2
- Και το PEAPv1/EAP-GTC

PEAPv0/EAP-MSCHAPv2

Το πρωτόκολλο PEAPv0/EAP-MSCHAPv2 ,είναι ο πλέον γνωστός σχηματισμός από τις κατηγορίες των PEAP πρωτοκόλλων , σε χρήση . Το εσωτερικό πρωτόκολλο πιστοποίησης που χρησιμοποιούν είναι το Microsoft Challenge Handshake Authentication πρωτόκολλο .
Μετά το EAP-TLS, το PEAPv0/EAP-MSCHAPv2 είναι το δεύτερο πιο ευρέως υποστηριζόμενο EAP πρωτόκολλο προτύπων στον κόσμο .

PEAPv1/EAP-GTC

Το PEAPv1/EAP-GTC πρωτόκολλο δημιουργήθηκε από την εταιρεία Cisco με σκοπό να παρέχει διαλειτουργικότητα μεταξύ των υπαρχόντων συμβολικών καρτών και των καταλόγων που βασίζονται στην επικύρωση των συστημάτων μέσω προστατευμένων καναλιών . Ακόμη κι αν η Microsoft σαν εταιρία συν-εφεύρεσαι το PEAP πρότυπο , δεν παρείχε ποτέ επιπρόσθετη υποστήριξη για το PEAPv1 , πράγμα που σημαίνει ότι το πρωτόκολλο PEAPv1/EAP-GTC δεν διαθέτει αυθεντική από το Windows OS τεχνική υποστήριξη .
Τόσο το πρωτόκολλο PEAPv0 όσο και το πρωτόκολλο PEAPv1 αναφέρονται στις μεθόδους της εξωτερικής επικύρωσης και είναι οι μηχανισμοί οι οποίοι δημιουργούν ένα ασφαλές TLS κανάλι για αν προστατέψουν τις επόμενες συναλλαγές επικύρωσης . Τα πρωτόκολλα EAP-MSCHAPv2, EAP-GTC και το EAP-TTLS αναφέρονται στις εσωτερικές μεθόδους επικύρωσης οι οποίες παρέχονται στον χρήστη ή στις συσκευές επικύρωσης .

EAP-FAST

Το πρωτόκολλο EAP – Flexible Authentication via Secure Tunneling , είναι ένα πρωτόκολλο το οποίο έχει προταθεί από την εταιρία Cisco ως αντικαταστάτης του πρωτοκόλλου LEAP . Το πρωτόκολλο αυτό δημιουργήθηκε με σκοπό να εξετάσει τις αδυναμίες του LEAP συντηρώντας την ¨ελαφριά¨ εφαρμογή . Η χρήση των πιστοποιητικών του server είναι προαιρετική στα πρωτόκολλα αυτού του τύπου . Τα EAP-FAST πρωτόκολλα χρησιμοποιούν προστατευμένα πιστοποιητικά πρόσβασης (Protected Access Credential-PAC) με σκοπό να καθιερώσουν μια TLS σήραγγα στην οποία τα πιστοποιητικά του πελάτη να ελέγχονται . Τα EAP-FAST χαρακτηρίζονται από τρείς φάσεις . Η φάση 0, είναι μια προαιρετική φάση στην οποία τα PAC μπορεί είτε να είναι χειροκίνητη είτε δυναμική . Τα PAC χρειάζεται να δημιουργηθούν μόνο μια φορά για το ζευγάρι RADIUS server , client .
Στην φάση 1 ,ο πελάτης και ο AAA server χρησιμοποιούν τα PAC για να καθιερώσουν το TLS τούνελ. Τέλος στην φάση 2 , τα πιστοποιητικά του πελάτη μεταδίδονται στην κρυπτογραφημένη σήραγγα.
Όταν είναι ενεργοποιημένη η αυτόματη παροχή των PAC ,τα EAP –FAST , παρουσιάζουν μια ευπάθεια στις επιθέσεις , μια επίθεση μπορεί να εμποδίσει το PAC παροδικά να μην μπορεί να χρησιμοποιήσει αυτό το συμβιβασμένο πιστοποιητικό του χρήστη . Αυτού του είδους η ευπάθεια μετριάζεται με την χρήση της χειροκίνητης παροχής των PAC ή με την χρησιμοποίηση πιστοποιητικών του server για την φάση της παροχής .
Υπάρχει ακόμη μια κατηγορία ευπάθειας , όπου ο AP hacker μπορεί να χρησιμοποιήσει το ίδιο SSID , απορρίπτοντας το PAC του χρήστη , και παρέχοντας ένα δικό του νέο. Οι περισσότεροι που κάνουν αίτηση μπορούν να τεθούν να προτρέπουν στον χρήστη να δεχτεί αυτό το νέο PAC , και στην περίπτωση που αυτός το δεχτεί , κατόπιν θα στείλει τα πιστοποιητικά του χρησιμοποιώντας την εσωτερική μέθοδος του χάκερ , ο οποίος στην συνέχεια θα πάρει ένα clear text κωδικό πρόσβασης (EAP-FAST w/GTC) ή θα επιχειρήσει μια τρωτή επίθεση λεξικών MSCHAPv2 hash.
Αξίζει να σημειωθεί ότι τα PAC αρχεία εκδίδονται σε μια βάση χρηστών . Έτσι εάν ένα νέος χρήστης συνδέεται στο δίκτυο μέσω μιας συσκευής , χρειάζεται ένα νέο PAC αρχείο να του παραχωρηθεί . Αυτός είναι και ένας λόγος για τον οποίον είναι δύσκολο να μην χρησιμοποιηθεί ένα EAP-FAST μέσα σε έναν μη ασφαλή ανώνυμο τρόπο παροχής . Η εναλλακτική λύση είναι να χρησιμοποιούνται οι κωδικοί πρόσβασης συσκευών αντ αυτού , αλλά ως αποτέλεσμα στην περίπτωση αυτή , δεν θα είναι ο χρήστης ο οποίος θα επικυρώνεται στο δίκτυο .

Τα EAP-FAST μπορούν να χρησιμοποιηθούν χωρίς τα PAC αρχεία , επιστρέφοντας πίσω στο κανονικό TLS .

EAP-SIM

Τα EAP για την ταυτότητα των συνδρομητών στο GSM (EAP for GSM Subscriber Identity) , χρησιμοποιούνται για την επικύρωση και την βασική διανομή συνόδου , χρησιμοποιώντας το Global System for Mobile Communication (GSM) Subscriber Identity Module (SIM).

EAP-AKA

Τέλος έχουμε τα πρωτόκολλα EAP-AKA , για την UMTS επικύρωση και την συμφωνία κλειδιού , τα οποία χρησιμοποιούνται για την επικύρωση και την διανομή κλειδιού συνόδου , χρησιμοποιώντας την Universal Mobile Telecommunication System (UMTS) Universal Subscriber Identity Module (USIM).

7.4.7.4.3 Remote Authentication Dial In User Service networking protocol (RADIUS).

Στα παραπάνω κεφάλαια έγινε αναφορά στο πρωτόκολλο RADIUS (Remote Authentication Dial In User Service networking protocol), καλό θα ήταν στο κομμάτι αυτό να αναλύσουμε λίγο αυτόν τον τύπο πρωτοκόλλου ο οποίο και σχετίζεται άμεσα με την διαδικασία της επικύρωσης .
Το πρωτόκολλο RADIUS είναι ένα πρωτόκολλο δικτύωσης το οποίο παρέχει συγκεντρωμένη διαχείριση πρόσβασης , έγκρισης και λογιστικής διαχείρισης , τόσο για τους ανθρώπους όσο και για τους υπολογιστές προκειμένου να συνδεθούν και να χρησιμοποιήσουν μια υπηρεσία δικτύου .
Όταν μια υπηρεσία ή μια συσκευή συνδέεται σε ένα δίκτυο απαιτείται επικύρωση αυτών . Τα δίκτυα ή οι υπηρεσίες που δεν απαιτούν την επικύρωση θεωρούνται ανοικτά ή ανώνυμα .
Μόλις ολοκληρωθεί η RADIUS επικύρωση , καθορίζονται με ποια προνόμια ή δικαιώματα είναι το πρόσωπο ή ο υπολογιστής εξουσιοδοτημένος , προκειμένου να έχουν πρόσβαση ή δικαίωμα εκτέλεσης αυτού του πόρου. Η υποστήριξη της Επικύρωσης , της Έγκρισης και της Λογιστικής διαχείρισης είναι γνωστή και με την ονομασία AAA διαδικασία .
Λόγω της ευρείας υποστήριξης και της πανταχού παρουσίας του πρωτοκόλλου RADIUS , χρησιμοποιείται συχνά από τα ISP, τα ασύρματα δίκτυα , τις ενσωματωμένες υπηρεσίες ηλεκτρονικού ταχυδρομείου , τα σημεία πρόσβασης , τις πόρτες δικτύου , τους Web server ή οποιονδήποτε άλλο προμηθευτή που χρειάζεται έναν καλά υποστηριζόμενο κεντρικό υπολογιστή AAA.

Περιγραφή της διαδικασίας AAA

Οι κεντρικοί υπολογιστές RADIUS χρησιμοποιούν την διαδικασία AAA με σκοπό να διαχειριστούν την πρόσβαση στο δίκτυο , ακολουθώντας δύο βασικά βήματα .
Στο πρώτο βήμα ο χρήστης ή η μηχανή στέλνει κάποιο αίτημα σε έναν server πρόσβασης δικτύου (NAS) για να αποκτήσει πρόσβαση σε έναν ιδιαίτερο πόρο δικτύων χρησιμοποιώντας πιστοποιητικά πρόσβασης . Τα πιστοποιητικά αυτά περνούν στην NAS συσκευή μέσω του πρωτοκόλλου σύνδεσης στρώματος . Για παράδειγμα , ένα PPP(Point –to- Point) πρωτόκολλο στην περίπτωση πολλών dialup ή DSL παροχέων .
Στην συνέχεια ο NAS , στέλνει ένα μήνυμα αιτήματος πρόσβασης στον RADIUS server , ζητώντας να του χορηγηθεί η έγκριση πρόσβασης μέσω του πρωτοκόλλου RADIUS . Αυτό το αίτημα συμπεριλαμβάνει τα πιστοποιητικά πρόσβασης , χαρακτηριστικά με την μορφή , ονόματος χρήστη και κωδικού πρόσβασης ή πιστοποιητικών ασφαλείας που παρέχονται από τον χρήστη .
Επιπλέον το αίτημα αυτό περιέχει τις πληροφορίες τις οποίες ο NAS γνωρίζει για τον χρήστη όπως η διεύθυνση δικτύων ή ο τηλεφωνικός αριθμός του και άλλες πληροφορίες σχετικές με το φυσικό σημείο σύνδεσης του χρήστη με τον NAS .
Στο δεύτερο βήμα ο RADIUS server ελέγχει ότι οι πληροφορίες είναι σωστές χρησιμοποιώντας μεθόδους επικύρωσης όπως τα PAP, τα CHAP ή τα EAP. Η απόδειξη του προσδιορισμού του χρήστη ελέγχεται , προαιρετικά , μαζί με τον έλεγχο των υπολοίπων πληροφοριών που είναι σχετικές με το αίτημα αυτό . Παλιά ο RADIUS server έλεγχε τις πληροφορίες του χρήστη σχετίζοντας τες με τις πληροφορίες που διέθετε μια βάση δεδομένων αρχείων . Οι σύγχρονοι RADIUS server , μπορούν ακόμη να το κάνουν αυτό ή μπορούν ακόμη να ανατρέξουν σε εξωτικές πηγές προκειμένου να γίνει ο έλεγχος των πιστοποιητικών αυτών .
Ο RADIUS server επιστρέφει στην συνέχεια μια από τις τρεις ακόλουθες απαντήσεις NAS , α)¨Απόρριψη-Nay ¨(απόρριψη πρόσβασης), β)¨Πρόκληση¨(πρόκληση πρόσβασης) , γ)¨Yea¨(αποδοχή πρόσβασης) .

- **Απόρριψη πρόσβασης :** Ο χρήστης αμφισβητείται και του απαγορεύεται χωρίς εξαίρεση η πρόσβαση σε όλους τους πόρους του δικτύου .

- **Πρόκληση πρόσβασης :** Ζητούνται από τον χρήστη πρόσθετες πληροφορίες , όπως ένας πρόσθετος κωδικός πρόσβασης , ή ένα PIN ή μια κάρτα . Η πρόκληση πρόσβασης χρησιμοποιείται επίσης στους πιο σύνθετους διαλόγους επικύρωσης , όπου ένα ασφαλή τούνελ καθιερώνεται μεταξύ της μηχανής των χρηστών και του server με τέτοιο τρόπο ώστε τα πιστοποιητικά πρόσβασης να είναι κρυμμένα από τον NAS.
- **Αποδοχή πρόσβασης :** Τέλος στην αποδοχή πρόσβασης , χορηγείται η πρόσβαση στον χρήστη . Μόλις επικυρωθεί ο χρήστης ο RADIUS server ελέγχει συχνά εάν ο χρήστης εξουσιοδοτείται για να μπορεί να χρησιμοποιεί την υπηρεσία δικτύων .Ένας δεδομένος χρήστης μπορεί να έχει την άδεια για να χρησιμοποιήσει το ασύρματο δίκτυο μιας επιχείρησης ,αλλά όχι την υπηρεσία VPN κα.

Ακόμη οι ιδιότητες της έγκρισης μεταβιβάζονται στον NAS , ο οποίος και ορίζει τους όρους της πρόσβασης που χορηγείτε
Για παράδειγμα οι ακόλουθες ιδιότητες έγκρισης μπορούν να περιληφθούν σε μια απάντηση Αποδοχής πρόσβασης .

- Η συγκεκριμένη IP address να ορίζεται στον χρήστη .
- Η περιοχή διευθύνσεων από την οποία θα έχει επιλεχθεί η IP του χρήστη .
- Το μέγιστο χρόνο που ο χρήστης μπορεί να παραμείνει συνδεδεμένος
- Ένας κατάλογος πρόσβασης , σειρά αναμονής προτεραιότητας ή άλλοι περιορισμοί που αφορούν την πρόσβαση ενός χρήστη .
- L2TP παράμετροι.
- VLAN παράμετροι.
- QoS παράμετροι.

7.4.7.4.4 Secure Shell protocol(SSH).

Το επόμενο πρωτόκολλο δικτύων που θα ασχοληθούμε είναι αυτό του SSH . Το πρωτόκολλο SSH-Secure Shell protocol , είναι ένα πρωτόκολλο το οποίο επιτρέπει στα στοιχεία μέσα σε ένα δίκτυο να ανταλλάσσονται χρησιμοποιώντας ένα ασφαλές κανάλι επικοινωνίας μεταξύ των δύο δικτυωμένων συσκευών που επιθυμούν να επικοινωνήσουν .
Χρησιμοποιείται κυρίως ,στα συστήματα που βασίζονται στα Linux και Unix, στην πρόσβαση των shell accounts, τα SSH δημιουργήθηκαν ακόμη ως αντικαταστάτες του TELNET και των άλλων μη ασφαλή απομακρυσμένων shells, τα οποία στέλνουν πληροφορίες , ειδικούς κωδικούς πρόσβασης και άλλες σημαντικές πληροφορίες , αφήνοντας τες ανοιχτές προς εκμετάλλευση . Η κρυπτογράφηση που χρησιμοποιείται από τα SSH παρέχει την εμπιστευτικότητα και την ακεραιότητα στα στοιχεία πέρα από ένα επισφαλές δίκτυο όπως είναι το Διαδίκτυο .
Τα SSH χρησιμοποιούν κρυπτογράφηση δημόσιου κλειδιού ,προκειμένου να πιστοποιούν τους απομακρυσμένους υπολογιστές ακόμη επιτρέποντας σε αυτόν να πιστοποιούν τους χρήστες εάν αυτό είναι αναγκαίο . Τα SSH χρησιμοποιούνται κυρίως για κάνουνε log on σε μια απομακρυσμένη μηχανή και να εκτελέσουμε σε αυτήν διάφορες εντολές , αλλά ακόμη

υποστηρίζουν το tunneling , προωθώντας της TCP ports και τις X11 συνδέσεις. Μπορούν τέλος να μεταφέρουν αρχεία χρησιμοποιώντας τα σχετικά πρωτόκολλα SFTP ή SCP.
Τα SSH χρησιμοποιούν το πρότυπο client-server. Ένας SSH server ακούει εξ ορισμού στις τυποποιημένες TCP πόρτες . Ένα SSH client πρόγραμμα τυπικά χρησιμοποιείται για ην εγκατάσταση των συνδέσεων σε ένα SSH daemon δεδομένου ότι αποδέχεται τις μακρινές συνδέσεις. Και ο SSH server και ο SSH client είναι παράγοντες στα περισσότερα σύγχρονα λειτουργικά συστήματα .

7.4.7.4.5 Secure Remote Password Protocol (SRP).

Τα Secure Remote Password Protocols είναι ένα πρωτόκολλο επικύρωσης με κωδικό πρόσβασης .
Τα πρωτόκολλα αυτά έχουν αρκετές θετικές ιδιότητες : όπως για παράδειγμα , επιτρέπουν σε έναν χρήστη να επικυρώνει αυτόνομα τον server , είναι αυθεντικά στις επιθέσεις λεξικών οι οποίες τοποθετούνται από τους λεγόμενους ¨ωτακουστές¨ , και δεν απαιτούν κάποιον τρίτο έμπιστο παράγοντα .
Η τυπική λειτουργία αυτών των πρωτοκόλλων είναι ότι μεταβιβάζουν αποτελεσματικά ένα κωδικό πρόσβασης μηδενικής γνώσης από τον χρήστη προς τον server . Μόνο ένας κωδικός πρόσβασης μπορεί να υποθέσει ανά προσπάθεια στην αναθεώρηση 6 του πρωτοκόλλου . Μια από τις πιο ενδιαφέρουσες ιδιότητες του πρωτοκόλλου αυτού είναι ότι ακόμα και αν ένας από τους δυο των κρυπτογραφημένων πρωτόκολλων και αν δεχτεί επίθεση , είναι ακόμη ασφαλή .Τα πρωτόκολλα SRP έχουν αναθεωρηθεί πολλές φορές , και αυτήν είναι η έκτη ανά περίοδος αναθεώρηση τους .
Τα SRP πρωτόκολλα δημιουργούν ένα μεγάλο ιδιωτικό κλειδί γνωστό στα δύο συμβαλλόμενα μέρη , κατόπιν ελέγχει αμφότερα τα συμβαλλόμενα μέρη ότι τα κλειδιά τους είναι ίδια και ότι και οι δύο πλευρές έχουν το ίδιο κωδικό πρόσβασης του χρήστη .
Στην περίπτωση που απαιτούνται κρυπτογραφημένες επικοινωνίες καθώς και η διαδικασία της επικύρωσης , το πρωτόκολλο SRP είναι ασφαλέστερο από το εναλλακτικό πρωτόκολλο SSH , και γρηγορότερο από ότι εάν χρησιμοποιούσαμε Diffie-Hellman με υπογεγραμμένα μηνύματα .

7.4.7.4.6 Ο όρος ¨CAPTCHA¨.

Ο όρος CAPTCHA , σχετίζεται άμεσα με την διαδικασία της επικύρωσης .Είναι ένας μηχανισμός δομικής πρόκλησης – απάντησης που χρησιμοποιείται στον τομέα των υπολογιστών για να εξασφαλίσει ότι η απάντηση δεν παράγεται από έναν υπολογιστή . Η διαδικασία περιλαμβάνει συνήθως (έναν server), ζητώντας από έναν χρήστη να συμπληρώσει μια απλή δοκιμασία την οποία ο υπολογιστής είναι σε θέση να παράγει και να βαθμολογήσει .
Επειδή οι υπολογιστές δεν είναι σε θέση να λύσουν τον CAPTCHA , οποιοσδήποτε χρήστης που εισάγει μια σωστή λύση αυτού , θεωρείται ανθρώπινος .
Κατά συνέπεια , περιγράφεται μερικές φορές ως αντίστροφο Turning test , επειδή διαχειρίζεται από μια μηχανή και στοχεύει σε κάποιον άνθρωπο , σε αντίθεση με το τυποποιημένο Turning test το οποίο διαχειρίζεται από έναν άνθρωπο και στοχεύει σε μια μηχανή .

Ένας κοινός τύπος CAPTCHA αποτελείται από σειρά από ψηφία που η εικόνα τους εμφανίζεται διαστρεβλωμένη στην οθόνη μας , τα οποία ψηφία ζητούνται να αναγνωριστούν από τους χρήστες .

Εικόνα 101: Παραδείγματα CAPTCHA .

Ο όρος CAPTCHA δημιουργήθηκε το 2000, και αποτελείται από τα αρχικά των ¨Completely Automated Public Turing test to tell Computers and Humans Apart¨.

7.4.7.4.7 Point of Access for Providers of Information (PAPI).

Τα PAPI (Point of Access for Providers of Information) είναι τα συστήματα που χρησιμοποιούνται για τον έλεγχο σε περιορισμένες πηγές πληροφοριών σε ολόκληρο το Διαδίκτυο . Βασικό μέλημα αυτών των συστημάτων είναι να κρατήσουν την λειτουργία της επικύρωσης σε τοπικό επίπεδο , όπου και ανήκει ο χρήστης , αφήνοντας τον πλήρη έλεγχο των πόρων στους ίδιους τους προμηθευτές τους.
Οι μηχανισμοί επικύρωσης σχεδιάζονται να είναι όσο το δυνατόν πιο εύκαμπτοι , επιτρέποντας σε κάθε επιχείρηση να χρησιμοποιεί το δικό της σχήμα επικύρωσης , διατηρώντας έτσι την ιδιωτικότητα των χρηστών , και τέλος προσφέροντας αρκετά στατιστικά στοιχεία και πληροφορίες στους προμηθευτές .
Επιπλέον οι μηχανισμοί επικύρωσης είναι διαφανείς ως προς τον χρήστη και το συμβατό σύστημα με τις πιο συχνά χρησιμοποιημένες μηχανές αναζήτησης Ιστού καθώς και οποιοδήποτε λειτουργικό σύστημα .
Το σύστημα αποτελείται από δύο ανεξάρτητα στοιχεία : τον **Server επικύρωσης (AS)** , και το **Σημείο Πρόσβασης (PoA)** . Αυτού του είδους η δομή καθιστά το τελικό σύστημα πιο εύκαμπτο και ικανό να ενσωματωθεί στα διάφορα περιβάλλοντα , καθώς δεν υπάρχει ανάγκη μιας-προς-μιας χαρτογράφησης μεταξύ του ASec και PoAs , αφού ένα δεδομένο PoA μπορεί να κατορθώσει να εξετάσει τα αιτήματα από οποιοδήποτε αριθμό ASes κατευθύνοντάς τα προς οποιονδήποτε αριθμό κεντρικών υπολογιστών δικτύου .

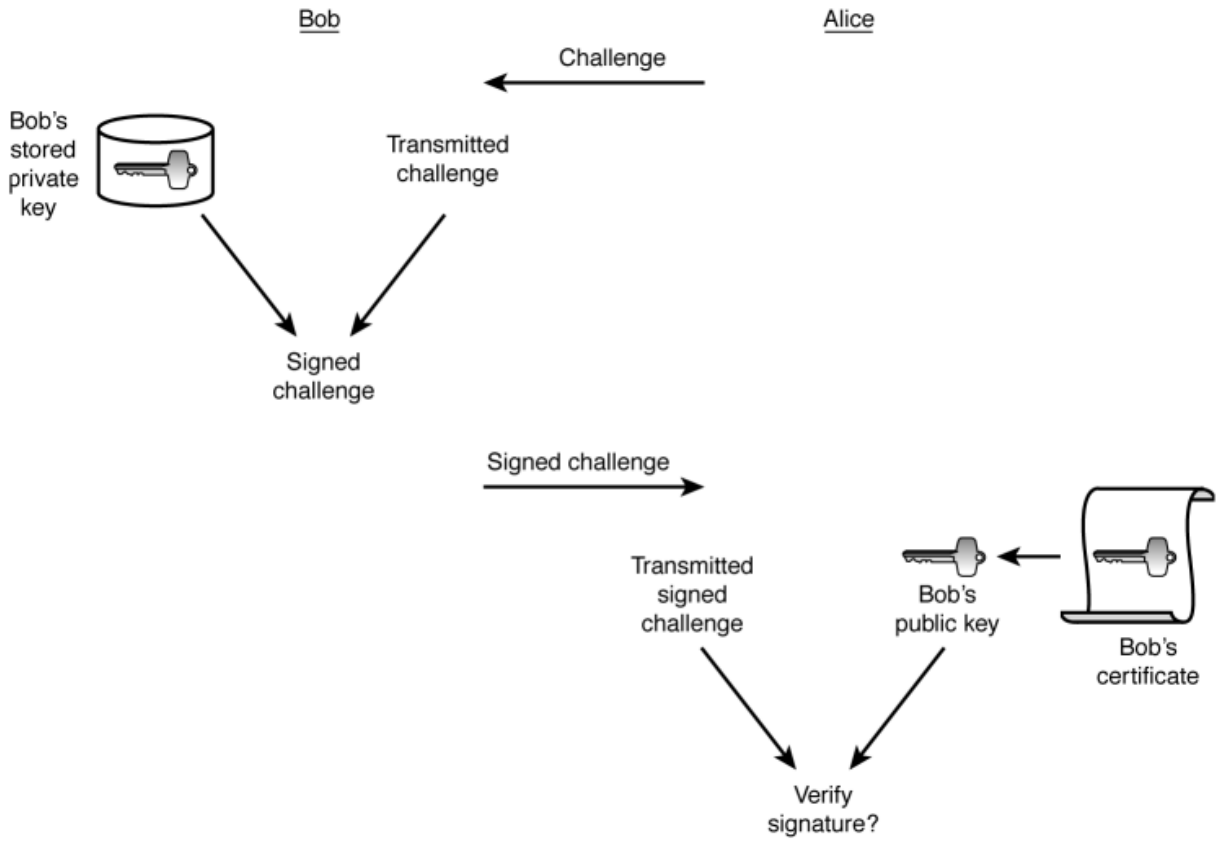
7.4.7.5 Πιστοποιητικό Δημόσιου κλειδιού (Public- key certificate).

Στην κρυπτογραφία , το **πιστοποιητικό δημόσιου κλειδιού(public key certificate ή identity certificate)** είναι ένα ηλεκτρονικό έγγραφο το οποίο ενσωματώνει μια ψηφιακή υπογραφή για να δεσμεύσει μαζί ένα δημόσιο κλειδί με μια ταυτότητα-πληροφορία για παράδειγμα όπως το όνομα ενός προσώπου ή ενός οργανισμού με την διεύθυνση τους κοκ . Το πιστοποιητικό αυτού του είδους μπορεί να χρησιμοποιηθεί για να ελέγξει ότι κάποιο συγκεκριμένο δημόσιο κλειδί ανήκει σε κάποιο άτομο .

Σε ένα χαρακτηριστικό σχέδιο υποδομής δημόσιου κλειδιού (PKI), η υπογραφή παίζει τον ρόλο της αρχής πιστοποιητικών (CA). Σε έναν έμπιστο Ιστό , η υπογραφή είναι είτε του ίδιου του χρήστη (αυτό υπογεγραμμένο πιστοποιητικό) , είτε άλλων χρηστών (¨επικυρώσεις¨). Σε κάθε μια από τις περιπτώσεις , η υπογραφή του πιστοποιητικού , είναι επιβεβαιώσεις από τον υπογράφοντα πιστοποιητικών ότι οι πληροφορίες ταυτότητας και το δημόσιο κλειδί του ανήκουν από κοινού .

7.4.7.5.1 Χρήση του πιστοποιητικού δημοσίου κλειδιού .

Τα πιστοποιητικά του δημοσίου κλειδιού , είναι χρήσιμα για τα μεγάλης κλίμακας δημόσιου κλειδιού συστήματα κρυπτογραφίας . Εξασφαλίζουν ασφαλή ανταλλαγή μυστικών κλειδιών μεταξύ των χρηστών , όσο αυτό γίνεται πρακτικά . Τα δημόσια κλειδιά κρυπτογραφίας παρέχουν έναν τρόπο να αποφεύγουμε αυτό το πρόβλημα.
Θα δώσουμε ένα παράδειγμα προκειμένου να γίνει κατανοητή αυτή η διαδικασία . Σε γενικές γραμμές έστω ότι η Alice επιθυμεί άλλο χρήστες να είναι σε θέση να της στέλνουν μυστικά μηνύματα , το μόνο που αυτή χρειάζεται να κάνει είναι να δημοσιεύσει το δημόσιο κλειδί της . Κάθε ένας χρήστης που επιθυμεί να της στείλει ασφαλής πληροφορίες , μπορεί να κρυπτογραφήσει τις πληροφορίες αυτές χρησιμοποιώντας το δημόσιο κλειδί της , γνωρίζοντας ότι μόνο η Alice μπορεί να αποκρυπτογραφήσει τις πληροφορίες αυτές χρησιμοποιώντας το αντίστοιχο ιδιωτικό της κλειδί .
Το μειονέκτημα είναι ότι έστω ο David ένας άλλος χρήστης , μπορεί να δημοσιεύσει ένα άλλο δημόσιο κλειδί , το οποίο είναι αυτός γνώστης του σχετικού ιδιωτικού του κλειδιού , και το οποίο δημόσιο κλειδί μπορεί να ισχυριστεί ότι είναι της Alice . Με αυτόν τον τρόπο ο David , μπορεί να εμποδίσει την Alice από το να διαβάσει κάποια από τα μηνύματα τα οποία προοριζόντουσαν για αυτήν .
Εάν όμως η Alice δημιουργούσε το δημόσιο κλειδί της μέσα σε ένα πιστοποιητικό , το οποίο και είχε υπογράψει ψηφιακά από έμπιστο φορέα , κάθε ένας που εμπιστεύεται τον φορέα αυτό θα γνώριζε εάν αυτό είναι το αυθεντικό δημόσιο κλειδί της.
Ένα άλλο παρόμοιο παράδειγμα , η Alice επιθυμεί να στείλει κάποια μηνύματα με τον Bob , αλλά η Alice μπορεί να μην έχει εξοικειωθεί με την αρχή πιστοποιητικών του Bob .Αυτό το σενάριο ισχύει όταν η έκδοση των πιστοποιητικών των δύο αυτών χρηστών έχει γίνει από διαφορετικούς φορείς . Στην περίπτωση λοιπόν αυτή μπορεί το πιστοποιητικό του Bob να περιλαμβάνει το δικό της CA δημόσιο κλειδί , που υπογράφεται από ένα ενός υψηλού επιπέδου CA2 το οποίο και ίσως να αναγνωρίζεται από την Alice . Αυτή η διαδικασία οδηγεί σε μια ιεραρχία των πιστοποιητικών , και σε πιο συνετές σχέσεις εμπιστοσύνης .



Εικόνα 102 : Επικοινωνία μέσω πιστοποιητικών δημόσιου κλειδιού .

7.4.7.6 Ενέργειες για πιο ασφαλείς συνδέσεις σε εξωτερικές προελεύσεις δεδομένων .

Όταν ορίζουμε μια σύνδεση σε μια εξωτερική προέλευση δεδομένων , όπως είναι μια σελίδα πρόσβασης δεδομένων , το περιβάλλον σύνταξης αποθηκεύει αυτές τις πληροφορίες ως κρυπτογραφημένη συμβολοσειρά σύνδεσης (απλό κείμενο) στη σελίδα HTML. Ως αποτέλεσμα, ένας χρήστης που ανοίγει την σελίδα χρησιμοποιώντας ένα πρόγραμμα περιήγησης μπορεί εύκολα αν δει την προέλευση HTML για την σελίδα και να διαβάσει τη συμβολοσειρά της σύνδεσης , η οποία μπορεί να περιλαμβάνει το όνομα χρήστη κα τον κωδικό πρόσβασης .

Με κύριο μέλημα μας λοιπόν, την ασφάλεια μας και θέλοντας να αποτρέψουμε τη μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες που λαμβάνονται από την συμβολοσειρά σύνδεσης . Αν η προέλευση δεδομένων υποστηρίζει αυτόν τον τρόπο ελέγχου ταυτότητας , χρησιμοποιούμε τον **μηχανισμό πιστοποίησης (Authentication) των Windows** (γνωστή επίσης και ως Αξιόπιστη σύνδεση και ενσωματωμένη ασφάλεια), η οποία χρησιμοποιεί τον λογαριασμό του τρέχοντος χρήστη των Microsoft Windows για σύνδεση σε μια εξωτερική προέλευση δεδομένων. Η χρήση της δυνατότητας πιστοποίησης των Windows για σύνδεση σε μια εξωτερική προέλευση δεδομένων έχει τα εξής πλεονεκτήματα :

- Δεν είναι απαραίτητο ο σχεδιαστής της σελίδας να εισάγει ένα όνομα χρήστη ή κάποιον κωδικό πρόσβασης για να συνδεθεί στην προέλευση δεδομένων, συνεπώς οι πληροφορίες αυτές δεν αποκαλύπτονται στην προέλευση της ιστοσελίδας .

- Δεν είναι απαραίτητο ο χρήστης της σελίδας να πληκτρολογήσει ένα όνομα χρήστη ή ένα κωδικό πρόσβασης για να συνδεθεί στην προέλευση δεδομένων όταν ανοίγει τη σελίδα , συνεπώς οι πληροφορίες αυτές δεν αποκαλύπτονται στην προέλευση της ιστοσελίδας .

- Μόνο σε έναν χρήστη λογαριασμού των Windows για τον οποίον έχουν οριστεί παράμετροι στο σύστημα ασφάλειας για την προέλευση δεδομένων θα επιτραπεί η σύνδεση με την εν λόγω προέλευση δεδομένων .

Στην συνέχεια θα δώσουμε ένα παράδειγμα προκειμένου να γίνουν κατανοητά όλα όσα προαναφέραμε .
Για παράδειγμα , έστω ότι επιθυμούμε να συνδεθούμε στον Microsoft SQL Server , με την δυνατότητα πιστοποίησης των Windows, τα βήματα που θα πρέπει να ακολουθήσουμε προκειμένου να το πετύχουμε αυτό είναι τα ακόλουθα :
Πριν μπορέσουμε να χρησιμοποιήσουμε την δυνατότητα πιστοποίησης των Windows για να συνδεθούμε σε μια βάση δεδομένων του Microsoft SQL Server, ο διαχειριστής του διακομιστή θα πρέπει να ορίσει τις ρυθμίσεις του διακομιστή ώστε να χρησιμοποιεί αυτό τον τρόπο ελέγχου ταυτότητας και θα πρέπει να παρέχει δικαίωμα σύνδεσης στο λογαριασμό του χρήστη μας των Windows (ή σε μια ομάδα στην οποία ανήκει ο λογαριασμό μας.) . Επιπρόσθετα , ο διαχειριστής διακομιστής θα πρέπει να παρέχει στον λογαριασμό μας ένα ελάχιστο επίπεδο δικαιωμάτων που απαιτούνται για την λίστα Συγκεντρωτικού Πίνακα .

1. Σε **Προβολή σελίδας**, μιας σελίδας πρόσβασης δεδομένων , κάνουμε κλικ στην επιλογή **Εργαλειοθήκη** της γραμμής εργαλείων .
2. Στην **Εργαλειοθήκη** , κάνουμε κλικ στο εργαλείο **Συγκεντρικός Πίνακας του Office** .
3. Κάνουμε κλικ στην λίστα Συγκεντρωτικού πίνακα για να την ενεργοποιήσουμε .
4. Κάνουμε κλικ στην εντολή **Εντολές και επιλογές** από την γραμμή εργαλείων και στην συνέχεια κάνουμε κλικ στην καρτέλα **Προέλευση δεδομένων**.
5. Κάνουμε κλικ στο κουμπί **Επεξεργασία** .
6. Στο παράθυρο διαλόγου Ιδιότητες **Data Link** , κάνουμε διπλό κλικ στην επιλογή **Υπηρεσίες .**
7. Στην καρτέλα **Σύνδεση** , καθορίζουμε το όνομα του διακομιστή .
8. Επιλέγουμε **Χρήση της ενσωματωμένης ασφάλειας των Windows** .
9. Επιλέγουμε μια βάση δεδομένων και κάνουμε κλικ στο κουμπί **Οκ**.

Εάν η δυνατότητα πιστοποίησης των Windows δεν είναι διαθέσιμη για την προέλευση δεδομένων στην οποία θέλουμε να συνδεθούμε , πρέπει να πληκτρολογήσουμε ένα όνομα χρήστη και έναν κωδικό πρόσβασης για να συνδεθούμε στην προέλευση δεδομένων . Έπειτα αυτό το όνομα χρήστη και ο κωδικός πρόσβασης μπορεί να είναι ορατά σε μια λίστα Συγκεντρωτικού Πίνακα , οποία θα βρίσκεται σε μια ιστοσελίδα . Καλό θα ήταν να μην χρησιμοποιούμε αυτόν τον τρόπο ελέγχου ταυτότητας για να συνδεθούμε σε ευαίσθητα δεδομένα από μια λίστα Συγκεντρωτικού Πίνακα ιστοσελίδας . Ακόμη και αν δεν μας ενδιαφέρει το γεγονός ότι μη εξουσιοδοτημένοι χρήστες θα μπορούν να δουν τα δεδομένα μας , θα πρέπει να συνδεόμαστε μόνο με ένα λογαριασμό χρήστη που έχει περιορισμένα δικαιώματα στην προέλευση δεδομένων . Για

παράδειγμα , όταν συνδεόμαστε σε μια βάση δεδομένων του SQL Server με ένα όνομα χρήστη και ένα κωδικό πρόσβασης , να μην χρησιμοποιούμε το λογαριασμό SA ή οποιοδήποτε άλλο λογαριασμό με υψηλό επίπεδο δικαιωμάτων , επειδή ένας μη εξουσιοδοτημένος χρήστης ενδεχομένως να μπορεί να χρησιμοποιήσει αυτό το λογαριασμό και τον κωδικό για να αποκτήσει πρόσβαση σε άλλα δεδομένα του διακομιστή .

7.4.7.7 Μηχανισμός Επικύρωσης των Microsoft Windows – Windows Genuine Authentication.

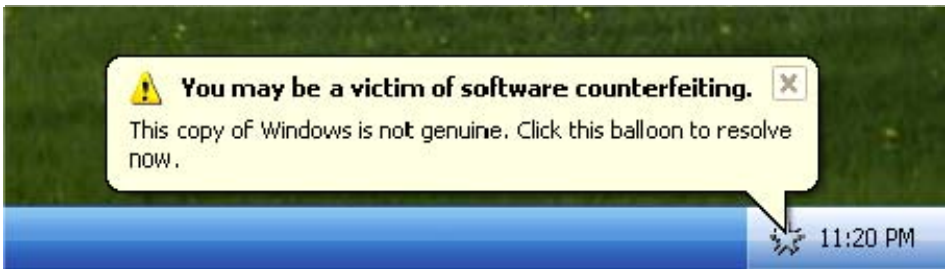
Εικόνα 103 : Μηχανισμός Genuine Microsoft software

Το Windows Genuine Authentication είναι η γνωστή εφαρμογή της Microsoft , μέσω της οποίας κάθε χρήστης θα πρέπει να επικυρώσει ότι το λειτουργικό σύστημα του είναι αυθεντικό , πριν κατεβάσει download , updates κ.α. Για να πραγματοποιηθεί ο έλεγχος αυθεντικότητας , θα πρέπει προηγουμένως τα Windows να έχουν ενεργοποιηθεί με ένα έγκυρο κλειδί .
Το WGA είναι ένα σύστημα αντί-πειρατείας που δημιουργήθηκε από την Microsoft , η οποία επιβάλλει σε απευθείας σύνδεση την επικύρωση διάφορων λειτουργικών συστημάτων της Microsoft , κατά την πρόσβαση τους σε διάφορες υπηρεσίες των Windows της Microsoft.
Το WGA υποστηρίζει τα λειτουργικά Windows XP , Windows Vista , δεν υποστηρίζει όμως παλαιότερα λειτουργικά αυτών όπως τα Windows 2000 ,Windows Server 2003 ή τα Windows 9X.
Η διαδικασία επικύρωσης WGA επικυρώνει την παρούσα εγκατάσταση των Windows και του κλειδιού αδειών της ενάντια στο σχετικό υλικό . Είναι προσβάσιμη σαν διαδικασία , από κάθε αυτόνομο πρόγραμμα και περιλαμβάνει τα εξής βήματα :

- Με την πρώτη επίσκεψη του χρήστη στην ιστοσελίδα του Microsoft Update , ο χρήστης λαμβάνει ένα μήνυμα , το οποίο του απαιτεί να επικυρώσει το αντίγραφο των Windows που διαθέτει μέσω κατεβάζοντας αρχικά την εφαρμογή ActiveX, η οποία και ελέγχει το κατά πόσο επικυρωμένο είναι το λειτουργικό . Εάν είναι επιτυχώς ολοκληρωμένη η επικύρωση των Windows , ο μηχανισμός αυτός αποθηκεύει ένα πρόσθετο αρχείο αδειών στο υπολογιστή για μελλοντική επικύρωση
- Μετά την επιτυχή διαδικασία της επικύρωσης η διαδικασία του κατεβάσματος των αναβαθμίσεων , συνεχίζεται κανονικά .

Εάν σε κάποια περίπτωση τα Windows δεν επικυρωθούν , δηλαδή αποδειχτεί ότι δεν έχουν μια έγκυρη άδεια , το WGA επιδεικνύει στον χρήστη μια συγκεκριμένη ειδοποίηση και αποτρέπει το κατέβασμα των μη κρίσιμων αναβαθμίσεων .

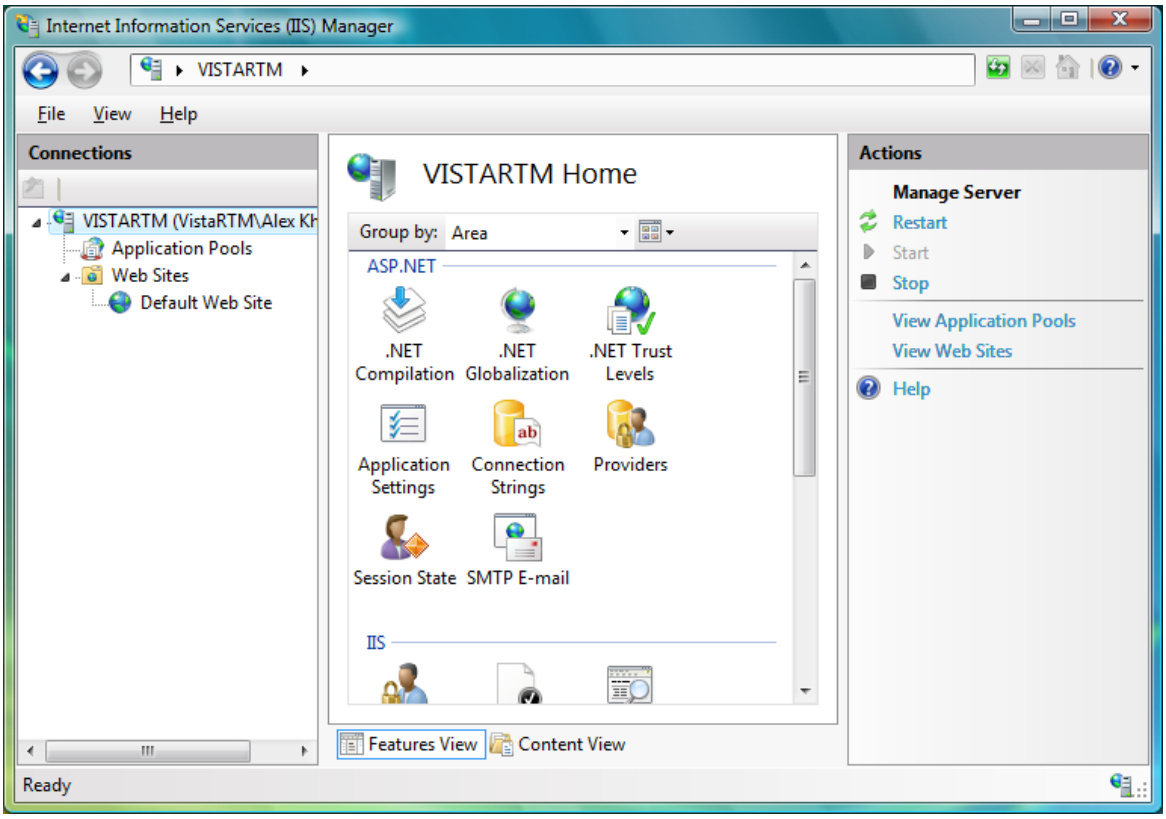
Στα Windows Vista , η αποτυχία επικύρωσης WGA ασκεί μεγαλύτερη επίδραση . Εκτός από την επίμονη ανακοίνωση προς τον χρήστη να θέσει εκτός λειτουργίας τις νέες μη κρίσιμες αναβαθμίσεις , ο μηχανισμός WGA θέτει εκτός λειτουργίας επίσης τις λειτουργίες των Windows, το Windows Aero , τον Windows Defender , Ready Boost . Στον χρήστη δίνεται μια περίοδος επιείκειας στην οποία και πρέπει να επικυρώσει το λειτουργικό του , εάν αυτός δεν το πραγματοποιήσει και με το πέρασμα του χρόνου όλο και μεγαλύτερο μέρος του λειτουργικού συστήματος τίθεται εκτός λειτουργίας και τα Windows λειτουργούν με μειωμένο τρόπο , στον οποίο έχει αφαιρεθεί το SP1 τωνWindows Vista .



Εικόνα 104 : Μήνυμα ειδοποίησης του μηχανισμού WGA.

7.4.7.8 Internet Information Services

Οι Internet Information Services (IIS) , στο παρελθόν αποκαλούμενος ως Internet Information Server , είναι ένα σύνολο υπηρεσιών βασισμένων στο Διαδίκτυο , το οποίο έχει παραχθεί από την Microsoft και προορίζεται για τους server που χρησιμοποιούν τα Windows . Είναι το δεύτερο στον κόσμο πιο δημοφιλές δίκτυο Ιστοχώρων κεντρικών υπολογιστών , από γενικής άποψης , πίσω από τον Apache HTTP Server . Οι server περιλαμβάνουν τελευταία , το FTP,SMTP,NNTP και HTTP/HTTPS .



Εικόνα 105 : Παράθυρο διαχείρισης των Internet Information Services (IIS).

Στο κεφάλαιο αυτό μελετάμε τον μηχανισμό της Επικύρωσης καθώς και τα συναφή με αυτήν προγράμματα και μεθόδους ασφαλείας . Αυτό λοιπόν που θα μας απασχολήσει και σε αυτό το σημείο είναι πως συνδέεται ο μηχανισμός της επικύρωσης με τις Internet Information Services .
Οι IIS παρέχουν ένα αριθμό από μηχανισμούς επικύρωσης προκειμένου να ελέγχουν την ταυτότητα του χρήστη , συμπεριλαμβανομένων ανώνυμων επικυρώσεων , της βασικής (based 64 encoded) επικύρωσης , της επικύρωσης αφομοιώσεων και της επικύρωσης που βασίζεται στα πιστοποιητικά των χρηστών .

7.4.7.9 Μηχανισμοί Επικύρωσης

Οι IIS έκδοσης 5 και πάνω υποστηρίζουν τους ακόλουθους μηχανισμούς επικύρωσης .

- Βασική πρόσβαση επικύρωσης.
- Επικύρωση πρόσβασης αφομοιώσεων.
- Ενσωματωμένη επικύρωση Windows.
- Επικύρωση .NET Passport.

Έκδοση 7 (IIS 7).

Η έκδοση 7 των IIS συμπεριλαμβάνεται τόσο στα Windows Vista όσο και στα Windows Server 2008, οι IIS χαρακτηρίζουν μια μορφωματική αρχιτεκτονική . Σε αντίθεση με έναν μονολιθικό κεντρικό υπολογιστή ο οποίος χαρακτηρίζει όλες τις υπηρεσίες , οι IIS7 διαθέτουν έναν πυρήνα

μηχανών κεντρικών υπολογιστών δικτύου . Οι ενότητες που προσφέρουν την συγκεκριμένη λειτουργία μπορούν να προστεθούν στην μηχανή αυτή και να εμφανίζουν τα χαρακτηριστικά γνωρίσματά της . Το πλεονέκτημα του να διαθέτεις αυτού του είδους την αρχιτεκτονική είναι ότι τα χαρακτηριστικά γνωρίσματα που απαιτούνται μπορούν να επιτραπούν και ακόμη ότι οι λειτουργίες μπορούν να επεκταθούν με την χρησιμοποίηση των ενοτήτων συνήθειας (custom modules) .
Οι IIS παρέχουν ένα σύνολο από ενότητες ,αλλά η Microsoft καταστεί διαδικτυακά και άλλες ενότητες απευθείας προσβάσιμες .Τα ακόλουθα σύνολα ενοτήτων ακολουθούν έναν server :

- **HTTP** Modules.
- **Security** Modules.
- Content Modules.
- **Compression** Modules.
- **Caching** Modules.
- **Logging και Diagnostic** Modules.

7.4.7.10 Επικύρωση Χρήστη μέσω χρήση του Amaranten Firewall.

Η επικύρωση του χρήστη , επιτρέπει στον διαχειριστή του συστήματος , να χορηγήσει ή να απορρίψει την πρόσβαση σε συγκεκριμένους χρήστες από τα συγκεκριμένες διευθύνσεις IP, οι οποίες είναι βασισμένες στα πιστοποιητικά των χρηστών .
Προτού να επιτραπεί οποιαδήποτε κυκλοφορία , για να περάσει μέσω οποιωνδήποτε επικυρωμένων κανόνων χρηστών, ο χρήστης πρέπει πρώτα από όλα να επικυρωθεί ο ίδιος . Το Amaranten firewall περνά κατά μήκος των πληροφοριών των χρηστών , σε ένα εξωτερικό κεντρικό υπολογιστή επικύρωσης , ο οποίος ελέγχει το χρήστη και το δεδομένο κωδικό πρόσβασης , και διαβιβάζει το αποτέλεσμα πίσω στο firewall.

Εάν η επικύρωση είναι επιτυχημένη , το Amaranten firewall θα θυμηθεί την διεύθυνση IP της πηγής του χρήστη , και οποιοιδήποτε κανόνες ταιριάζουν με την επικύρωση του χρήστη , θα επιτραπούν . Συγκεκριμένοι κανόνες μπορούν να καθοριστούν οι οποίοι έχουν να κάνουν με την επικύρωση του χρήστη , και αφήνοντας έτσι τους κανόνες οι οποίοι δεν επηρεάζουν άμεσα την επικύρωση του χρήστη .
Το Amaranten Firewall υποστηρίζει το RADIUS (Remote Authentication Dial In User Service) πρωτόκολλο επικύρωσης. Αυτό το πρωτόκολλο χρησιμοποιείται σε πολλά σενάρια , όπου η επικύρωση των χρηστών απαιτείται , είτε από αυτό το ίδιο είτε ως αρχής –τέλους σε άλλες υπηρεσίες επικύρωσης .
Αυτήν την περίοδο υπάρχουν δύο βασικοί agent επικύρωσης που υποστηρίζονται , ο HTTP και ο XAUTH . Και τους δύο θα τους εξηγήσουμε λεπτομερώς παρακάτω.

7.4.7.10.1 User Authentication Servers configuration.

Οι servers που χρησιμοποιούνται με την επικύρωση χρηστών , καθορίζονται στο τμήμα User Authentication Servers configuration , που βρίσκεται στο Miscellaneous φάκελο .

Γενικοί παράμετροι

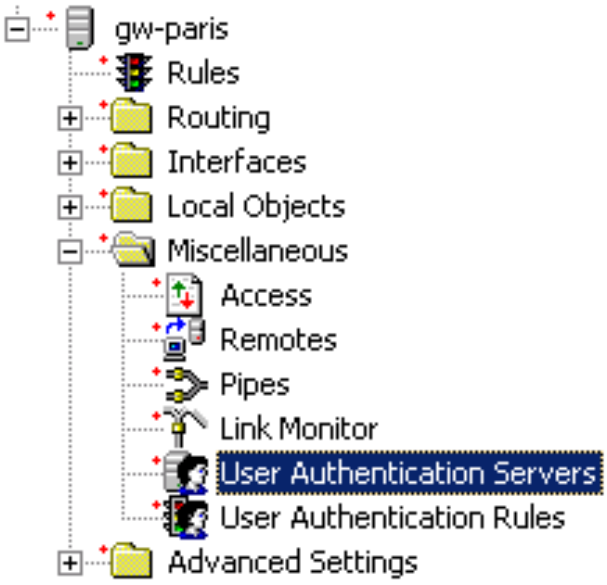
Name: Συμβολικό όνομα του επικυρωμένου server.

Type: Ο τύπος του server επικύρωσης που χρησιμοποιείται. Αυτήν την περίοδο υποστηρίζεται μόνο ο τύπος RADIUS υποστηρίζεται .

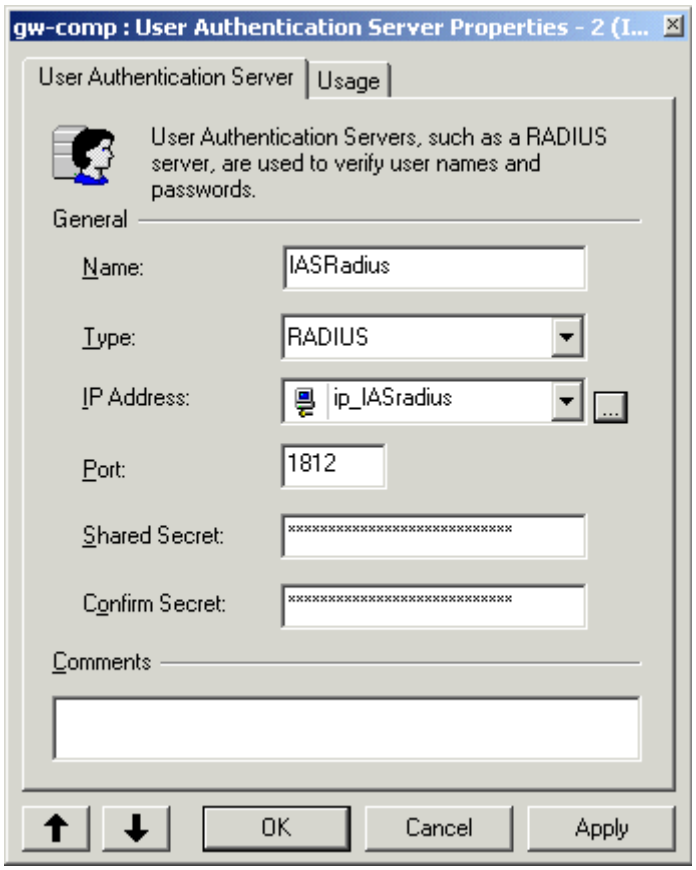
IP Address: IP Address, η το συμβολικό όνομα εάν ο κεντρικός υπολογιστής έχει καθοριστεί προηγουμένως στον host και το τμήμα δικτύου, του κεντρικού υπολογιστή επικύρωσης
Port: Η πόρτα του επικυρωμένου server.

Shared Secret: Το shared Secret επιτρέπει την βασική κρυπτογράφηση του κωδικού πρόσβασης του χρήστη, όταν διαβιβάζεται το RADIUS –packet από το firewall στον RADIUS server. Το shred secret είναι έναν μικρό κεφάλαιο , μπορεί να περιέχει μέχρι 100 χαρακτήρες , και πρέπει να δακτυλογραφηθεί ακριβώς το ίδιο και στο firewall και στο RADIUS server .

Confirm Secret: Το Confirm Secret επιβεβαιώνει ότι το shares secret έχει εισαχθεί σωστά, με τον να το εισάγει πάλι.



Εικόνα 106 :User Authentication Servers configuration.



Εικόνα 107 : Ρύθμιση του User Authentication Server.

7.4.7.10.2 User Authentication Rules configuration.

Οι κανόνες επικύρωσης διευκρινίζουν από πού οι χρήστες έχουν άδεια για να επικυρώσουν στο firewall.Επιτρέπουν επίσης στον διαχειριστή του firewall να καθορίσει , διαφορετικούς χρονικούς περιορισμούς και η επικύρωση των servers βασίζεται στην πηγή του επικυρωμένου χρήστη . Επιπλέον οι κανόνες επικύρωσης χρηστών δίνουν την δυνατότητα της προσαρμογής στο βλέμμα της επιστροφής μηνυμάτων από το firewall στον επικυρωμένο χρήστη (για παράδειγμα μηνύματα όπως : επιτυχία σύνδεσης , σύνδεση αποτυχημένη και άλλα ανάλογα με την πηγή του χρήστη).

Γενικοί παράμετροι

Name: Συμβολικό όνομα του κανόνα.

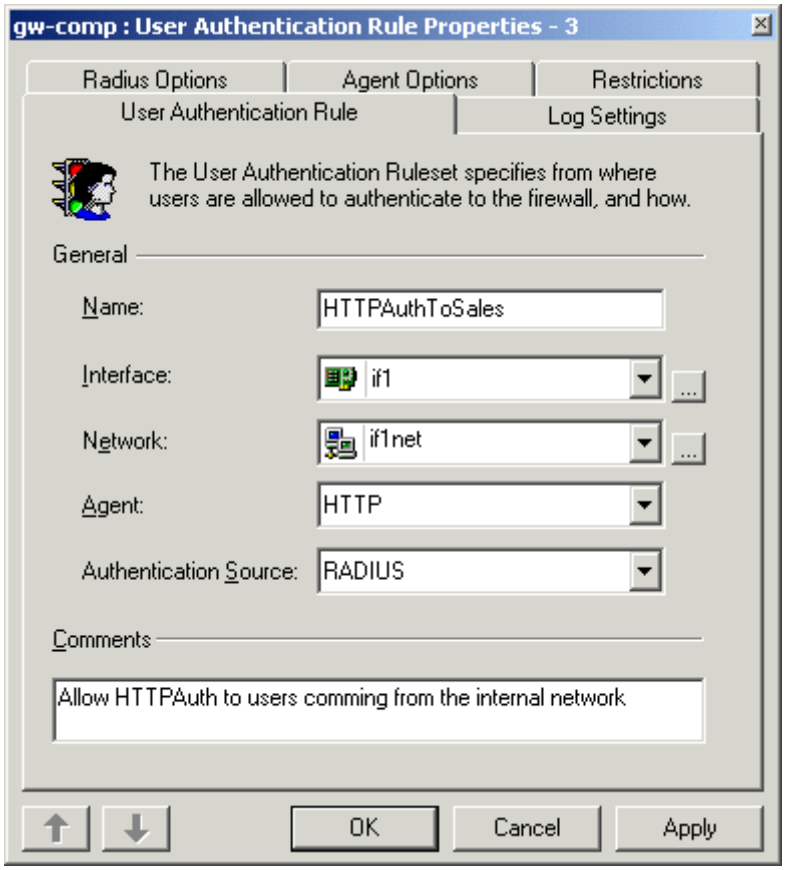
Interface: Το Interface, στο οποίο λαμβάνει χώρα η σύνδεση.

Network: Το αντικείμενο δικτύων ότι η εισερχόμενη διεύθυνση IP πρέπει να ένα μέρος

Agent: HTTP ή XAUTH.

- **HTTP**, ο χρήστης επικυρώνεται με το πρώτο σερφάρισμα που κάνει στο firewall, στην πύλη (port) 80, με έναν internet browser και έπειτα εισάγεται στα πιστοποιητικά του χρήστη.
- **XAUTH,** ο χρήστης θα προτραπεί για ένα username και ένα password, κατά την καθιέρωσης μιας VPN σήραγγας (εάν η σήραγγα έχει διαμορφωθεί για να απαιτείσει την επικύρωση XAUTH).

Authentication source: RADIUS ή DISALLOW, επιλέγουμε DISALLOW για να απορρίψει συγκεκριμένα οποιεσδήποτε προσπάθειες επικύρωσης για τον συγκεκριμένο χρήστη.



Εικόνα 108 : Παράθυρο ρυθμίσεων Κανόνων Επικύρωσης Χρήστη .

7.4.7.10.3 Επιλογές RADIUS.

Όταν επιλέγεται να χρησιμοποιηθεί η μέθοδος RADIUS για την επικύρωσης που χρησιμοποιείται για την κρυπτογράφηση του κωδικού πρόσβασης των χρηστών, το πακέτο , στέλνεται από το firewall στον RADIUS server . Αυτό μπορεί να ρυθμιστεί από την επιλογή του PAP ή του CHAP .

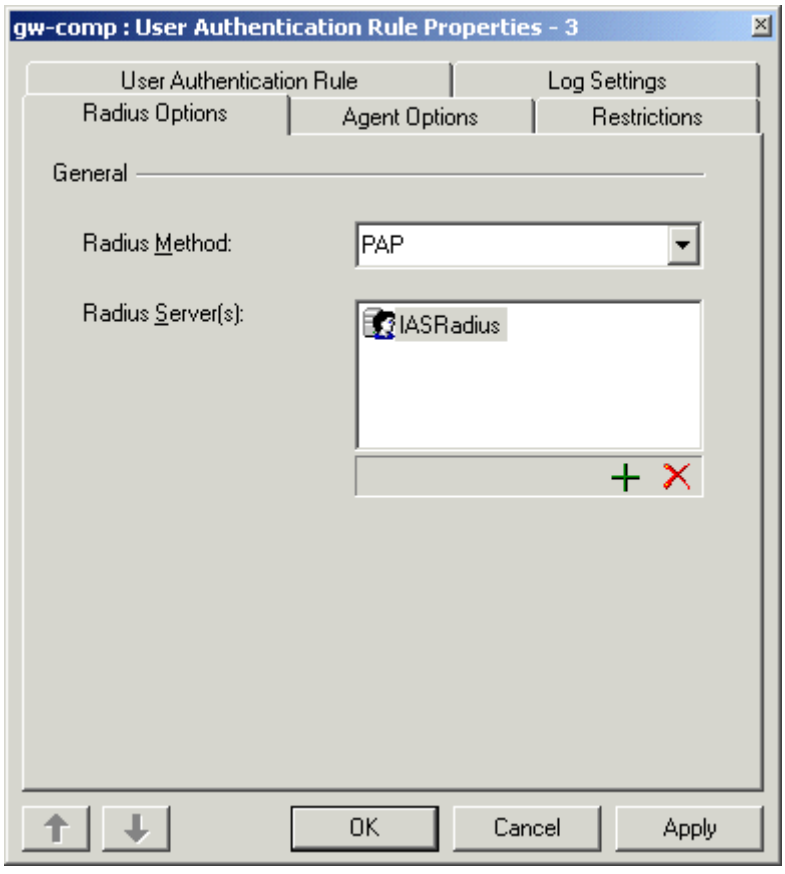
Γενικοί παράμετροι

PAP: Password Authentication Protocol , ίσως θεωρείται το λιγότερο ασφαλές από τα δύο . Εάν κάποιο πακέτο RADIUS παρεμποδιστεί καθώς μεταδίδεται μεταξύ του firewall και του RADIUS

server , ο κωδικός πρόσβασης του χρήστη μπορεί να εξαχθεί , λαμβάνοντας υπόψη το χρόνο . Η άλλη πλευρά σε αυτό είναι ότι ο κωδικός πρόσβασης δεν είναι απαραίτητο να αποθηκευτεί στο plain text στον server του RADIUS .

CHAP: Challenge Handshake Authentication Protocol .Δεν επιτρέπει σε έναν μακρινό επιτιθέμενο να εξάγει τον κωδικό πρόσβασης χρηστών από ένα παρεμποδισμένο πακέτο RADIUS . Εντούτοις , ο κωδικός πρόσβασης πρέπει να αποθηκευτεί στο plain text του RADIUS server .

Authentication Servers: Ένας κατάλογος κεντρικών υπολογιστών επικύρωσης που χρησιμοποιούνται για να επικυρώσουν τους χρήστες που ταιριάζουν με αυτόν τον κανόνα . Αυτοί οι servers θα πρέπει αρχικά να έχουν οριστεί στην περιοχή του User Authentication Servers . Εάν μια απάντηση δεν παραλαμβάνεται από τον πρώτο server στον κατάλογο , το firewall συνεχίζει με τον επόμενο ,και ούτω καθεξής ,έως ότου είτε να παραληφθεί μια απάντηση , ή να τελειώσει ο κατάλογος των servers . Το firewall θα χρησιμοποιήσει τον πρώτο server που θα επιστρέψει μια απάντηση (είτε αυτή είναι χορήγηση πρόσβασης , είτε είναι άρνηση πρόσβασης) , την επόμενη φορά που αυτός ο κανόνας χρησιμοποιηθεί . Αφού επαναρυθμιστεί , ο πρώτος server στον κατάλογο θα χρησιμοποιηθεί πάλι . Ένα μέγιστο των τριών servers επικύρωσης , μπορεί να διαμορφωθεί ανά κανόνα επικύρωσης χρηστών .



Εικόνα 109 : Παράθυρο RADIUS Options

7.4.7.10.4 Agent Options.

Γενικοί παράμετροι

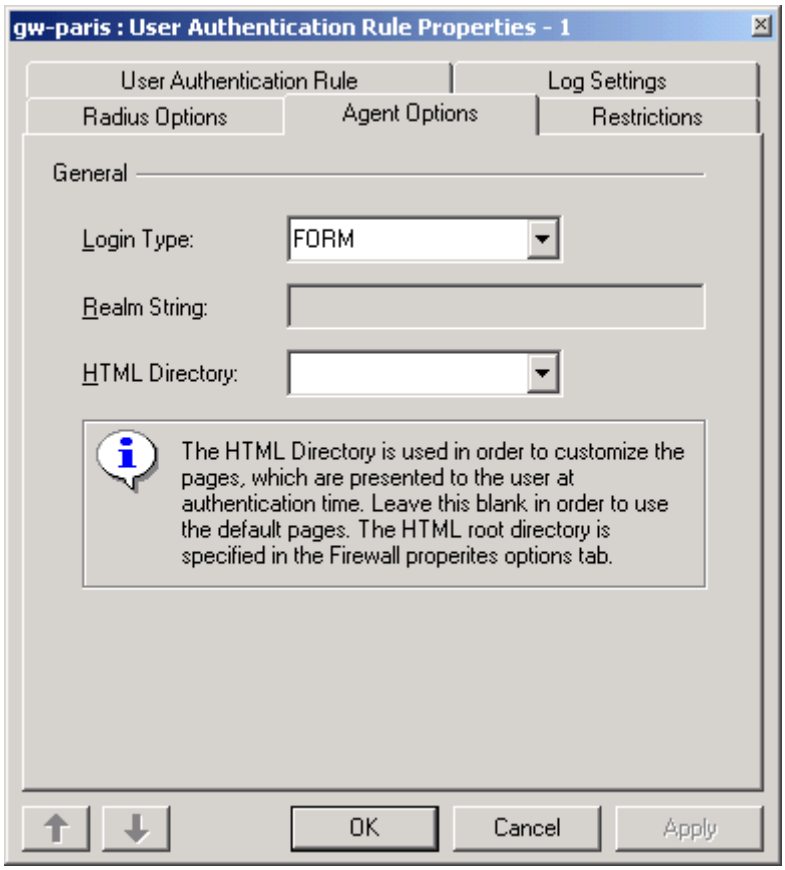
Login Type: FORM ή BASICAUTH.

- **FORM**, θα παρουσιαστεί στον επικυρωμένο χρήστη, μια HTML σελίδα, η οποία θα περιλαμβάνει μια HTML-FORM καθώς θα σερφάρει στο Internet. Αυτή η φόρμα περιέχει δύο πεδία , ένα για το όνομα χρήστη και ένα για τον κωδικό πρόσβασης . Αυτές οι τιμές θα στέλνονται στην συνέχεια στο firewall με την χρήση της μεθόδου POST.

- **BASICAUTH,** στον τύπο αυτό, δεν παρουσιάζεται στον χρήστη καμία HTML σελίδα, αλλά αντίθετα του εμφανίζεται ένα 401 Authentication-Required πλαίσιο διαλόγου. Το πρόβλημα με τον BASICAUTH τύπο είναι ότι οι μηχανές αναζήτησης του Ιστού , εναποθηκεύουν το όνομα χρήστη και τον προσωπικό κωδικό που πληκτρολογούμε στο 401 Authentication-Required πλαίσιο διαλόγου . Αυτό κανονικά δεν είναι πρόβλημα εάν η μηχανή αναζήτησης είναι κλεισμένη ,δεδομένου ότι καθαρίζει την cache στην συνέχεια , αλλά για τα συστήματα των οποίων η μηχανή αναζήτησης συναρμολογείται στο λειτουργικό σύστημα , η cache είναι πολύ δυσκολότερο να καθαριστεί .

Realm string – Η συμβολοσειρά αυτή παρουσιάζεται ως κομμάτι του 401 – Authentication-Required μηνύματος , το οποίο παρουσιάζεται στον χρήστη όταν αυτός σερφάρει στο Internet .Η εξ ορισμού τιμή του είναι Protected Resources . Αυτή η ρύθμιση ισχύει μόνο για τον τύπο σύνδεσης BASICAUTH.

HTML Directory – Αυτό χρησιμοποιείται με σκοπό να προσαρμοστεί το βλέμμα των σελίδων που παρουσιάζονται στον χρήστη στον χρόνο επικύρωσης. Καλύτερα είναι να αφήνουμε το πεδίο κενό προκειμένου να χρησιμοποιηθεί η σελίδα προεπιλογής .



Εικόνα 110 : Παράθυρο ρυθμίσεων Agent Options .

7.4.7.10.5 Περιορισμοί.

Timeouts.

Idle Timeout - Εάν ένας χρήστης έχει επικυρωθεί επιτυχώς, και δεν έχει ανιχνευτεί καμία κυκλοφορία από την διεύθυνσή IP του, για αυτόν τον αριθμό των δευτερολέπτων που ορίζουμε στο πεδίο αυτό, θα αποσυνδεθεί αυτόματα.

Session Timeout – Εάν ένα χρήστης έχει επικυρωθεί επιτυχώς, θα αποσυνδεθεί μετά από αυτά τα πολλά δευτερόλεπτα που έχουν καθοριστεί στο πεδίο αυτό, ανεξάρτητα από το εάν το firewall έχει δει δραστηριότητα από τον χρήστη ή όχι.

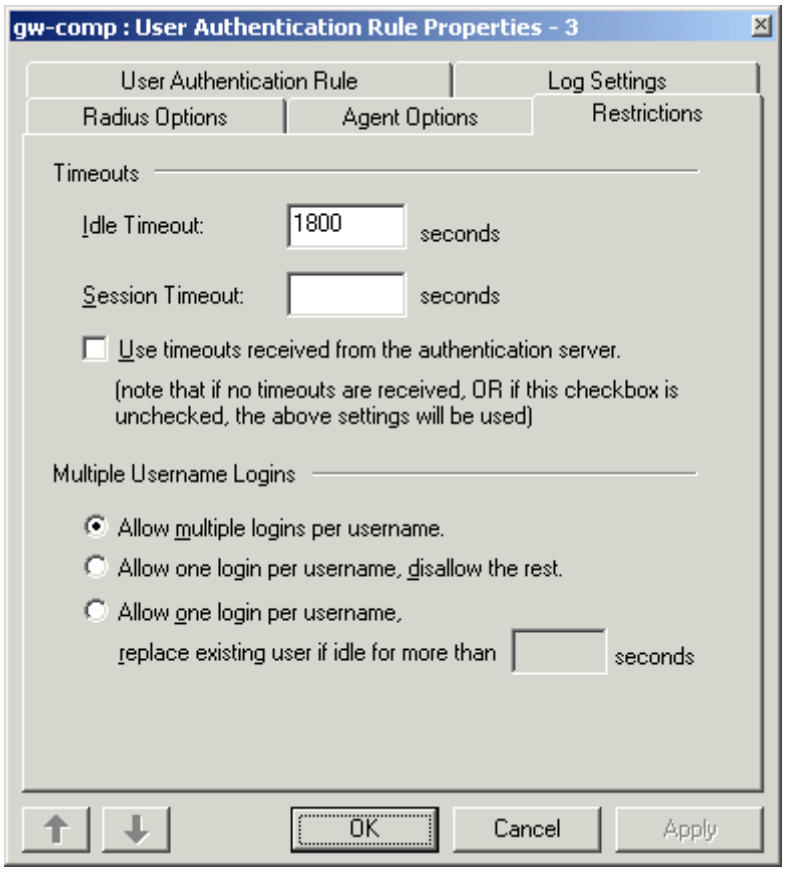
Use timeouts received from the authentication server – Κάποιοι server επικύρωσης, όπως για παράδειγμα ο RADIUS , μπορούν να ρυθμιστούν έτσι ώστε να επιστρέφουν session – idle timeouts τιμές. Εάν αυτό το πλαίσιο είναι επιλεγμένο , το firewall θα προσπαθήσει να χρησιμοποιήσει αυτούς τους timeouts , πριν από τις τιμές των timeouts ορίζονται παρακάτω από αυτό . Εάν δεν λαμβάνονται timeouts από τον server επικύρωσης , ή αν αυτό το κουτί δεν είναι επιλεγμένο , θα χρησιμοποιηθούν οι τιμές των timeouts που βρίσκονται παρακάτω από αυτό το πλαίσιο .

Multiple Username Logins.

Allow multiple logins per username: Εάν αυτό το πλαίσιο είναι επιλεγμένο, το firewall θα επιτρέψει σε χρήστες από διαφορετικές πηγές διευθύνσεων IP, αλλά με το ίδιο όνομα χρήστη, να είναι ταυτόχρονα συνδεδεμένοι.

Allow one login per username, disallow the rest: Εάν αυτό το πλαίσιο είναι επιλεγμένο, το firewall θα επιτρέψει σε έναν μόνο χρήστη με κάποιο συγκεκριμένο όνομα χρήστη να συνδεθεί. Δηλαδή εάν ένας χρήστης από μια άλλη διεύθυνση IP επιχειρήσει να επικυρωθεί με το ίδιο όνομα χρήστη , με έναν ίδιο δηλαδή όνομα χρήστη με κάποιου ήδη επικυρωμένου χρήστη , το firewall θα απαγορεύσει την πραγματοποίηση της σύνδεσης αυτής .

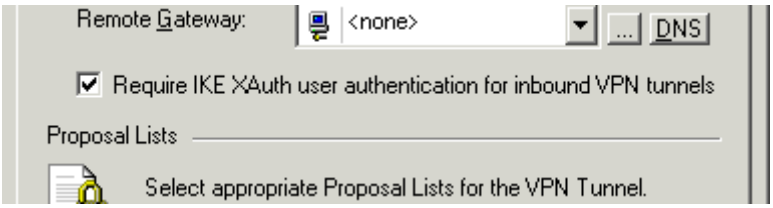
Allow one login per username, replace existing user if idle for more than x seconds: Εάν αυτό το πλαίσιο είναι επιλεγμένο, το firewall θα επιτρέψει σε έναν μόνο χρήστη με κάποιο συγκεκριμένο όνομα χρήστη να συνδεθεί. Εάν ένας χρήστης από μια άλλη διεύθυνση IP προσπαθήσει να επικυρωθεί με το ίδιο όνομα χρήστη ,με αυτό που ανήκει σε κάποιον ήδη επικυρωμένο χρήστη , το firewall θα ελέγξει εάν ο επικυρωμένος χρήστης έχει προβεί σε κάποια ενέργεια τα τελευταία χ δευτερόλεπτά (όπου χ η τιμή που έχει τοποθετηθεί μέσα στο πλαίσιο αυτό). Σε αυτήν την περίπτωση , δηλαδή εάν είναι ανενεργός για περισσότερα από τα χ δευτερόλεπτα , ο παλιός χρήστης θα απομακρυνθεί , και ο νέος χρήστης θα συνδεθεί . Εάν όχι , το αίτημα για νέα σύνδεση , θα απορριφθεί .



Εικόνα 111 :Παράθυρο ρυθμίσεων Περιορισμών .

7.4.7.10.6 Ενεργοποιώντας το XAUTH μέσα σε VPN τούνελ .

Σε ένα πλαίσιο ενός VPN τούνελ , όταν είναι επιλεγμένο το κουτάκι με την τίτλο Require IKE XAuth user authentication for inbound VPN tunnel είναι ενεργοποιημένο το XAUTH .

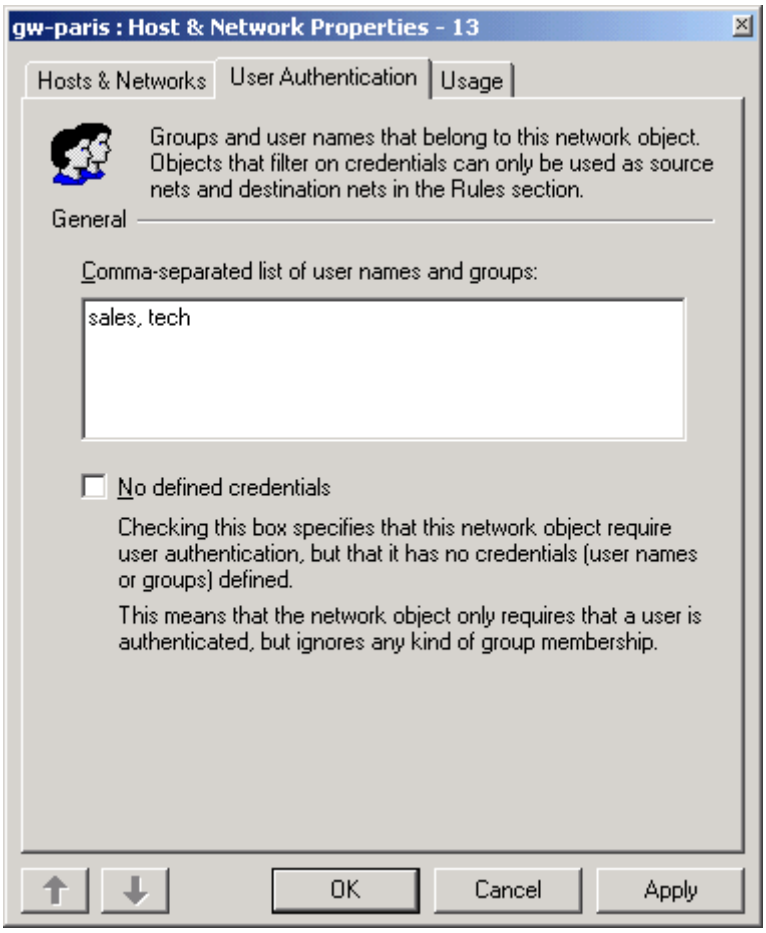


Εικόνα 112 : Παράθυρο επιλογή ενεργοποίησης XAUTH , σε ένα VPN τούνελ .

Προκειμένου να χρησιμοποιηθεί το XAUTH μέσα σε ένα VPN tunnel , ένας κανόνας επικύρωσης χρηστών που διευκρινίζει το XAUTH σαν τύπο agent , θα πρέπει να δημιουργηθεί . Σημειώνουμε ότι για XAUTH , το firewall δεν αποθηκεύει την περίοδο αυτή , καμία από τις πληροφορίες του επικυρωμένου χρήστη , όπως για παράδειγμα την πηγή της διεύθυνσης IP , ή τα timeouts . Η επιλογή χρησιμοποιείται μόνο για να καθιερώσει το VPN τούνελ .

7.4.7.10.7 Ενεργοποιώντας τα αντικείμενα δικτύων που απαιτούν την επικύρωση των χρηστών .

Προκειμένου να δημιουργηθούν οι συγκεκριμένοι κανόνες επικύρωσης χρηστών , οι πληροφορίες επικύρωσης των χρηστών , εισάγονται στα αντικείμενα δικτύων . Τα ονόματα των χρηστών και οι μεμονωμένοι χρήστες που ανήκουν σε αυτό το αντικείμενο δικτύου ,διευκρινίζονται εδώ . Αυτά τα αντικείμενα δικτύων ,μπορούν στην συνέχεια να χρησιμοποιηθούν στο πεδίο του κανόνα , σαν τους κανονικούς κανόνες . Οι ίδιες πληροφορίες των γκρουπ , θα πρέπει να επιστρέφονται από τον RADIUS server , χρησιμοποιώντας την ιδιότητα του Amaranten – User-Group , όπως εξηγήσαμε νωρίτερα .
Τέλος επιλέγοντας το κουτάκι No defined credentials, διευκρινίζεται ότι αυτό το αντικείμενο δικτύου , απαιτεί την επικύρωση χρηστών , αλλά δεν διαθέτει κανένα όνομα χρήστη ή δεν διευκρινίζεται η ομάδα χρηστών του . Αυτό σημαίνει ότι το αντικείμενο δικτύου απαιτεί μόνο να είναι επικυρωμένος ο χρήστης , αγνοώντας οποιοδήποτε είδος ομάδας χρηστών και αν ανήκει .



Εικόνα 113 : Παράθυρο ενεργοποίησης επικύρωσης χρηστών , στα αντικείμενα δικτύου .

7.4.7.10.8 Ενεργοποιώντας τους κανόνες που απαιτούν την επικύρωση των χρηστών .

Οι κανόνες που απαιτούν την επικύρωση των χρηστών , δημιουργούνται ακριβώς όπως δημιουργούνται οποιοιδήποτε άλλοι κανόνες με εξαίρεση ότι τα αντικείμενα των χρηστών περιέχουν τις πληροφορίες επικύρωσης των χρηστών , που δημιουργούνται όπως προαναφέραμε προηγουμένως .

	Name	Action	Secure	Pipes	Log	Source Inter	Source Network	Destination Ir	Destination Ne	Service	Comments
1	MembersPOP3	Allow	☐		☐	if1	Members	any	all-nets	TCP All -> 110	allow POP3 for members
2	MailToMembers	Allow	☐		☐	any	all-nets	if1	Members	TCP All -> 25	Members may run SMTP servers

Εικόνα 114 : Παράθυρο ενεργοποίησης κανόνων που απαιτούν την επικύρωση των χρηστών .

Σημειώνουμε ότι η πρόσβαση στην port 80 στο firewall , πρέπει να προσδιορίζεται για τους επικυρωμένους χρήστες , οι οποίοι χρησιμοποιούν το HTTP πρότυπο ως τύπο agent .

Όταν το firewall έχει να κάνει με έναν κανόνα που απαιτεί την επικύρωση χρηστών στο αντικείμενο δικτύων πηγής , πρέπει να τελούνται τα εξής :

1. Το firewall ελέγχει ποια ομάδα και /ή ονόματα χρηστών , περιέχουν την πηγή του αντικειμένου του δικτύου για αυτόν τον κανόνα .
2. Το firewall έπειτα σιγουρεύεται ότι ένα χρήστης από την διεύθυνση IP , από την οποία προήλθε η κυκλοφορία που προκάλεσε τον κανόνα αυτόν , επικυρώνεται αυτήν την περίοδο . Εάν δεν βρεθεί κανένας επικυρωμένος χρήστης , ο κανόνας δεν θα ενεργοποιηθεί .
3. Εάν βρεθεί κάποιος επικυρωμένος χρήστης , το firewall συγκρίνει της πληροφορίες τις οποίες έχει συλλέξει από το βήμα 1 με τις πληροφορίες του γκρουπ/ονόματος χρήστη του επικυρωμένου χρήστη .
4. Εάν ο επικυρωμένος χρήστης απαιτεί τα πιστοποιητικά από το αντικείμενο δικτύων της πηγής σε αυτόν τον κανόνα ,ο κανόνας προκαλείται , Εάν όχι ο κανόνας δεν προκαλείται .

Όταν το firewall αντιμετωπίζει έναν κανόνα που απαιτεί την επικύρωση χρηστών στο αντικείμενο δικτύων προορισμού , πρέπει να γίνονται οι ίδιες ενέργειες με την προηγούμενη περίπτωση και να εκτελούνται τα βήματα 1 έως 4 .

7.5 *DRM Digital Rights Management.*

Τα DRM (Διαχείριση ψηφιακών δικαιωμάτων) είναι το αγγλικό ακρωνύμιο για τη διαχείριση ψηφιακών δικαιωμάτων. Το DRM είναι μια τεχνολογία ελέγχου πρόσβασης που χρησιμοποιείται από τους εκδότες και τους κατόχους πνευματικών δικαιωμάτων και γενικά τις υπηρεσίες παροχής περιεχομένου, όπως τα ηλεκτρονικά καταστήματα, για να ελέγχουν τον τρόπο διανομής των αρχείων μουσικής και βίντεο που λαμβάνουμε και ακόμη για να περιορίσουν τη χρήση των ψηφιακών μέσων ή των συσκευών ηλεκτρονικά καταστήματα πωλούν και νοικιάζουν τραγούδια και ταινίες στα οποία έχει εφαρμοστεί η τεχνολογία DRM.

Ο όρος χρησιμοποιείται για να περιγράψει οποιαδήποτε τεχνολογία αποτρέπει την αναρμόδια χρήση των μέσων ή των συσκευών, και γενικά δεν συμπεριλαμβάνει άλλους τύπους προστασίας αντιγραφής οι οποίοι μπορούν να παρακαμφθούν χωρίς να τροποποιήσουν αισθητά τα μέσα ή την αντίστοιχη συσκευή , παραδείγματα αυτών είναι οι serial number ή τα key files . Μπορούμε ακόμη με τον όρο αυτόν να αναφερθούμε στους περιορισμούς που συνδέονται με τις συγκεκριμένες περιπτώσεις ψηφιακών εργασιών ή συσκευών .
Ο όρος αυτός μπορεί ακόμη να παραπέμψει σε περιορισμούς που εφαρμόζονται και συνδέονται με ορισμένες περιπτώσεις ψηφιακών εργασιών ή ακόμη και συσκευών. Τα DRM , επικαλύπτουν με την προστασία αντιγράφων λογισμικού (copy protection) ως ένα βαθμό. Εντούτοις ο όρος DRM εφαρμόζεται συνήθως στα δημιουργικά μέσα (ταινίες, μουσική κτλ.) σε αντίθεση με την προστασία αντιγράφων λογισμικού που τείνει να αναφέρεται στους μηχανισμούς προστασίας αντιγράφων στο λογισμικό υπολογιστών.

Η ψηφιακή διαχείριση δικαιωμάτων δημιουργήθηκε και χρησιμοποιείται σε ικανοποιητικό βαθμό από τις προμηθευτικές επιχειρήσεις όπως η Sony, η Apple Inc, η Microsoft και η BBC, ακόμη και ο Windows Media Player, καθώς και τα περισσότερα ηλεκτρονικά καταστήματα και οι νέες συσκευές, υποστηρίζουν ή χρησιμοποιούν τη διαχείριση ψηφιακών δικαιωμάτων (Windows Media Digital Rights Management 10 - DRM 10).

Υπάρχει όμως και η αντίθετη όψη του νομίσματος , η χρήση της ψηφιακής διαχείρισης δικαιωμάτων είναι αμφισβητούμενη .Κάποιο ποσοστό των χρηστών υποστηρίζουν ότι είναι απαραίτητο , για τους κατόχους των πνευματικών δικαιωμάτων , η χρήση της ψηφιακής διαχείρισης δικαιωμάτων . Υπάρχει και ένα άλλο όμως ποσοστό χρηστών , οι οποίοι υποστηρίζουν ότι η χρήση της λέξης ¨δικαιώματα¨ είναι παραπλανητική . Η θέση την οποία υποστηρίζουν είναι ότι κάτοχοι των πνευματικών δικαιωμάτων , προσπαθούν να περιορίσουν την χρήση του υλικού τους στους τρόπους οι οποίοι δεν καλύπτονται από τους υφιστάμενους νόμους . Το ηλεκτρονικό συνοριακό ίδρυμα καθώς και οι άλλοι αντίπαλοι της , θεωρούν τα συστήματα DRM ανταγωνιστικές πρακτικές,

Στην πράξη όλα τα ευρέως χρησιμοποιημένα DRM συστήματα έχουν νικηθεί ή έχουν παρακαμφθεί όταν επεκτείνεται σε πολλούς πελάτες . Ο περιορισμός αντιγραφής του ακουστικού και του οπτικού υλικού είναι ιδιαίτερα δύσκολος στην ύπαρξη της analog hole , και υποστηρίζεται ότι αποτελεσματικό DRM είναι λογικά αδύνατο να υπάρξει λόγω αυτού του λόγου που προαναφέραμε .

7.5.1 Τεχνολογίες όπου χρησιμοποιείται η DRM

Οι τεχνολογίες της ψηφιακής διαχείρισης δικαιωμάτων προσπαθούν να ελέγξουν την χρήση των ψηφιακών μέσων , παρεμποδίζοντας την πρόσβασή σε αυτά ,την αντιγραφή ή την μετατροπή τους σε άλλους τύπους αρχείων από τους χρήστες . Πολύ πριν από την άφιξη των ψηφιακών ή ακόμα και των ηλεκτρονικών μέσων , οι κάτοχοι των πνευματικών δικαιωμάτων , οι ικανοποιημένοι παραγωγοί, ή οι άλλοι οικονομικά ή καλλιτεχνικά ενδιαφερόμενοι , είχαν τις νομικές αντιρρήσεις πάνω στο κομμάτι της αντιγραφής των τεχνολογιών .
Η εμφάνιση στην συνέχεια των ψηφιακών μέσων και των αναλογικών/ψηφιακών τεχνολογιών μετατροπής , ειδικά αυτών που χρησιμοποιούνται στην μαζική αγορά γενικής χρήσης προσωπικών υπολογιστών , έχουν αυξήσει απέραντα τις ανησυχίες των εξαρτωμένων οργανώσεων ή του εξαρτώμενου ατόμου ειδικά σε τομείς όπως μέσα στην μουσική ή την βιομηχανία κινηματογράφου .
Από την μια τα αναλογικά μέσα τα οποία χάνουν πλέον αναπόφευκτα την ποιότητα τους σε κάθε γενιά αντιγραφών , και σε μερικές περιπτώσεις ακόμη και κατά τη διάρκεια της κανονικής χρήσης , από την άλλη τα ψηφιακά αρχεία μέσων μπορούν ακόμη να αναπαράγουν έναν απεριόριστο αριθμό φορών τους χωρίς την υποβάθμιση στην ποιότητα τους όπως γίνεται με τις επόμενες αντιγραφές στα αναλογικά αρχεία.
Η εμφάνιση των προσωπικών υπολογιστών ως οικιακές συσκευές , έχει καταστήσει ικανό στους χρήστες να μετατρέπουν τα μέσα (τα οποία μπορούν ή αυτά τα οποία δεν μπορούσαν) , αρχικά σε μια φυσική / αναλογική μορφή ή σε μια μορφή ραδιοφωνικής μετάδοσης , τα μετατρέπουν σε μια παγκόσμια ψηφιακή μορφή (η διαδικασία αυτή καλείται ripping) για την θέση ή για το time shifting , συνδυάζοντας την έτσι με το Διαδίκτυο καθώς και με τα δημοφιλή εργαλεία file sharing . Η νέα τους

αυτή μορφή τα καθιστά πιο επιρρεπή κάνοντας την αναρμόδια διανομή των αντιγράφων των ψηφιακών μέσων (η οποία αποκαλείται ψηφιακή πειρατεία) πολύ ευκολότερη .
Στην πραγματικότητα , οι εξαρτώμενες επιχειρήσεις των μέσων ή οι ιδιοκτήτες αυτών , θεωρούν κάθε καταναλωτή ,ο οποίος διαθέτει σύνδεση στο Διαδίκτυο , ως πιθανό κόμβο ενός δικτύου διανομής που θα μπορούσε να χρησιμοποιηθεί για να διανείμει τα αναρμόδια αντίγραφα . Αν και οι τεχνικοί έλεγχοι στην αναπαραγωγή και την χρήση του λογισμικού έχουν χρησιμοποιηθεί περιοδικά από την δεκαετία του 70 , ο όρος ¨DRM¨ έχει αρχίσει να σημαίνει αρχικά την χρήση αυτών των μέτρων ελέγχου του καλλιτεχνικού λογοτεχνικού περιεχομένου .
Οι τεχνολογίες DRM έχουν επιτρέψει στους εκδότες να επιβάλουν τις πολιτικές πρόσβασης που όχι μόνο απαγορεύουν τις παραβιάσεις των πνευματικών δικαιωμάτων , αλλά και αποτρέπουν την νόμιμη και δίκαιη χρήση των εργασιών ή ακόμη εφαρμόζουν τους περιορισμούς χρήσης άλλα όχι επάνω στις εργασίες που διανέμονται . Παραδείγματα περιλαμβάνουν την εφαρμογή του DRM πάνω σε συγκεκριμένα public-domain ή σε ανοιχτής άδειας ηλεκτρονικά βιβλία , ή ακόμη η DRM περιλαμβάνεται σε ηλεκτρονικές συσκευές των πελατών και εφαρμόζεται σε εργασίες αυτών .
Συνηθέστερα η DRM χρησιμοποιείται από την βιομηχανία της ψυχαγωγίας (π.χ. ταινίες, βίντεο κτλ) ,έχει όμως βρει χρήση και σε άλλες καταστάσεις.

7.5.1.1 DRM και Video.

Ένα πρόωρο παράδειγμα ενός συστήματος DRM είναι το **Content Scrambling System (CSS)** , το οποίο χρησιμοποιήθηκε από το DVD Forum στις ταινίες DVD από το 1996 περίπου .Το CSS χρησιμοποίησε έναν απλό αλγόριθμο κρυπτογράφησης , και απαιτούσε από τους κατασκευαστές των συσκευών να υπογράψουν τις συμφωνίες αδειών οι οποίες περιόριζαν τα χαρακτηριστικά γνωρίσματα τους , όπως τα ψηφιακά αποτελέσματα που θα μπορούσαν να χρησιμοποιηθούν για να εξάγουν τα υψηλής ποιότητα ψηφιακά αντίγραφα ταινιών . Κατά συνέπεια, το μόνο καταναλωτικό υλικό το οποίο ήταν ικανό να αποκωδικοποιήσει τις ταινίες DVD ελεγχότανε , και αν και έμμεσα , από το forum DVD , το οποίο περιόριζε την χρήση των μέσων DVD σε άλλα συστήματα .
Τα Windows Vista περιέχουν ένα σύστημα DRM το οποίο αποκαλείται Protected Media Path , και το οποίο περιέχει το Protected Video Path (PVP) . Το PVP προσπαθεί να σταματήσει το DRM-περιορισμένο περιεχόμενο από το να χρησιμοποιηθεί κατά την διάρκεια που ένα μη εγκεκριμένο πρόγραμμα τρέχει, με σκοπό να εμποδίσει την πρόσβαση αυτού του μη εγκεκριμένου προγράμματος στο περιεχόμενο αυτό. Επιπλέον το PVP μπορεί να κρυπτογραφήσει τις πληροφορίες κατά την διάρκεια της μετάδοσης , στην οθόνη ή στην κάρτα γραφικών , η οποία το καθιστά δυσκολότερο να κάνει μη εγκεκριμένες εγγραφές .
Το DRM σχετίζεται και με άλλες λειτουργίες , όπως με την Advance Access Content System(AACS) ένα σύστημα DRM το οποίο σχετίζεται με τα HD DVD και τα Blu-Ray Disc.
Εμείς όμως θα αναλύσουμε το κομμάτι που σχετίζεται με τα Windows Vista και το οποίο όπως προαναφέραμε ονομάζεται Protect Media Path.

7.5.1.2 Protect Media Path.

Το Protect Media Path είναι ένα σύνολο από τεχνολογίες που δημιουργούν ένα ¨¨Προστατευμένο περιβάλλον ¨ , το οποίο αρχικά έχει συμπεριληφθεί στο λειτουργικό σύστημα των Windows Vista και το οποίο χρησιμοποιείται με σκοπό να εφαρμόσει την ψηφιακή διαχείριση δικαιωμάτων (DRM 10) στο περιεχόμενο . Τα υποσύνολα αυτών των τεχνολογιών είναι το Protected Video Path – PVP και το Protected User Mode Audio –PUMA .

Το προστατευμένο περιβάλλον στο οποίο το DRM περιεχόμενο παίζεται περιέχει τα τμήματα μέσων που παίζουν το περιεχόμενο DRM , έτσι η εφαρμογή πρέπει μόνο να παρέχει τον τηλεχειρισμό , αντί να πρέπει να αντιμετωπίσει τα μη προστατευμένα δεδομένα του περιεχομένου . Το προστατευμένο περιβάλλον παρέχει επίσης όλη την απαραίτητη υποστήριξη για τους τρίτους παράγοντες οι οποίοι είναι εγκεκριμένοι από την Microsoft . Παρέχει τέλος , ένα ¨τοίχος ¨ενάντια στην εξωτερική αντιγραφή , όπου αντίθετα μέσα στους τοίχους , το περιεχόμενο αυτό μπορεί να υποβληθεί σε επεξεργασία από τους χρήστες χωρίς να καταστείτε διαθέσιμο προς επεξεργασία στο μη εγκεκριμένο λογισμικό .
Προκειμένου να αποτραπούν οι χρήστες από την αντιγραφή του περιεχομένου DRM, τα Windows Vista παρέχουν την διαδικασία της απομόνωσης η οποία ελέγχει συνεχώς ποιο λογισμικό kernel-mode φορτώνεται . Εάν κάποιο ανεπιβεβαίωτο συστατικό ανιχνευτεί τα Vista , σταματάνε την εκτέλεση του DRM περιεχομένου . Το προστατευμένο περιβάλλον εφαρμόζεται ολοκληρωτικά στο λογισμικό .
Αυτοί οι περιορισμοί απασχολούν τις διάφορες εξωτερικές πηγές του υπολογιστή. Για το DRM περιεχόμενο οι ψηφιακές εξωτερικές πηγές όπως το **Digital Visual Interface (DVI)** ,ή το **High-Definition Multimedia Interface (HDMI)**, θα έχουν **High-bandwidth Digital Content Protection (HDCP)** , για να αποτρέψουν κάποιον από το να αντιγράψει τα ψηφιακά stream .
Ακόμη και τα αναλογικά πρότυπα TV, τυπικά απαιτούν μερικούς περιορισμούς , οι οποίοι παρέχονται από μηχανισμούς όπως τον Macro vision και το CGMS-A . Αυτοί οι περιορισμοί ισχύουν μόνο για το DRM περιεχόμενο , όπως τα HD DVD και τα Blu-Ray Disc τα οποία και κρυπτογραφούνται με AACS , και ισχύουν επίσης στα Windows XP χρησιμοποιώντας τις υποστηριζόμενες εφαρμογές αναπαραγωγής ήχου . το τυποποιημένο μη προστατευμένο περιεχόμενο του χρήστη δεν θα βρίσκεται αντιμέτωπο με αυτούς τους περιορισμούς. Υπάρχουν όμως και μερικοί μη συμβατοί τύποι παραγωγής , όπως ο S/PDIF (Sony/Philips Digital Interchange Format) τα οποία και δεν ταιριάζουν με την τεχνολογία DRM 10 , και οι οποίοι μηχανισμοί θα πρέπει για τον λόγο αυτό , να τεθούν εκτός λειτουργίας , εάν το περιεχόμενο διευκρινίζεται έτσι .
Στα Windows Vista , ο έλεγχος των τηλεοπτικών εξωτερικών πηγών παρέχεται από την PVP-OPM , η οποία είναι ουσιαστικά η επόμενη γενιά των Certified Output Protection Protocols(COPP) τα οποία είχαν παρουσιαστεί στα Windows XP .

Η τεχνολογία DRM εμφανίζεται και σε άλλους τομείς , όπως στην μουσική , στα ηλεκτρονικά βιβλία , και ακόμη και στα έγγραφα .

7.5.2 Νόμοι σχετικοί με την DRM .

Τα ψηφιακά συστήματα διαχείρισης δικαιωμάτων έχουν λάβει διεθνή νομική υποστήριξη μετά την εφαρμογή της Συνθήκης Πνευματικών Δικαιωμάτων WIPO το 1996 (WCT) .Κάποιο από τα άρθρα της συνθήκης απαιτεί την συμβολή των μελών εθνών , στην θέσπιση συνθηκών και νόμων ενάντια σε αυτούς που παρακάμπτουν τον DRM μηχανισμό .
Το WCT έχει εφαρμοστεί στα περισσότερα κράτη μέλη της παγκόσμιας οργάνωσης πνευματικής ιδιοκτησίας .

7.5.3 Windows Media DRM .

Το Windows Media είναι μια υπηρεσία ψηφιακής διαχείρισης δικαιωμάτων για την πλατφόρμα Windows Media . Είναι σχεδιασμένο να παρέχει ασφαλή παράδοση του ακουστικού και του οπτικού περιεχομένου πάνω σε ένα δίκτυο IP σε έναν υπολογιστή ή σε κάποια άλλη συσκευή αναπαραγωγής ήχου , με τέτοιο τρόπο ώστε ο διανομέας να μπορεί να ελέγχει ανά πάσα στιγμή τον τρόπο με τον οποίο χρησιμοποιείται το περιεχόμενό του.
WMDRM περιλαμβάνει τα ακόλουθα συστατικά:

- Windows Media Rights Manager (WMRM) SDK για το packaging των δεδομένων και την έκδοση αδειών.
- Windows Media Format SDK (WMF SDK) για την οικοδόμηση των εφαρμογών των Windows που υποστηρίζουν DRM και Media τύπους.
- Windows Media DRM for Portable Devices (WMRM-PD) για την υποστήριξη μη συνδεδεμένων φορητών συσκευών αναπαραγωγής ήχου.
- Windows Media DRM for Network Devices (WMRM-ND) για την προστασία της ροής των περιεχομένων σε συσκευές που συνδέονται με ένα εγχώριο δίκτυο.

7.5.3.1 Πως λειτουργεί το Windows Media DRM.

Τον Μάιο του 2007 η Microsoft δημοσίευσε το πρωτόκολλο δικτύων πίσω από τον μηχανισμό αποκτήσεων αδειών . Σύμφωνα με την ανακοίνωση αυτή ,το λογισμικό του πελάτη λαμβάνει έναν 7 – bytes κλειδί περιεχομένου plain text από τον server αδειών . Ο server κρυπτογραφεί το κλειδί πριν το μεταφέρει στον πελάτη , με ένα κοινό 160-bit ECC κλειδί . Ο server , στέλνει επίσης ένα ID του κλειδιού του περιεχομένου , αυτό είναι μη κρυπτογραφημένο . Ο πελάτης στην συνέχεια χρησιμοποιεί το κρυπτογραφημένο κλειδί ,για αποκρυπτογραφεί το εξουσιοδοτημένο ρεύμα μέσων .
Σαν anti-spoofing μέτρο , τα πρόσθετα πεδία όπως τα δικαιώματα αναπαραγωγής ήχου και ο τυχαίος αριθμός , κρυπτογραφούνται με τρία επιπλέον προκαθορισμένα βασικά ζευγάρια κλειδιών , είτε από το λογισμικό του πελάτη είτε από αυτού του server.

- KC client software ECC key pair.
- KM client machine ECC key pair.
- KS server software ECCkey pair.

Το Windows Media DRM , σχεδιάστηκε να είναι ανανεώσιμο , δηλαδή σχεδιάστηκε με την προϋπόθεση ότι θα υποστεί ρωγμή και θα πρέπει έτσι συνεχώς να ανανεώνεται από την ,Microsoft .
Γενικά αυτά τα είδη των ρωγμών λειτουργούν όλα με τον ίδιο τρόπο μέχρι ένα σημείο .Παρά ότι σπάνε την κρυπτογράφηση την ίδια , η οποία είναι ανέφικτη , αυτές οι ρωγμές γαντζώνουν ή παρεμποδίζουν το τμήμα του περιεχομένου των ¨μαύρων κουτιών ¨ καθώς αυτά τρέχουν πετώντας έξω τα κλειδιά ή το ίδιο το περιεχόμενο από την μνήμη .Αυτών των ειδών οι τεχνικές αντιμετωπίζονται από την Microsoft μέσω των αυτοματοποιημένων αναπροσαρμογών Windows , τις οποίες στην συνέχεια ο χρήστης μπορεί να διαλέξει ξεχωρίζοντας αυτές που επιθυμεί και ακυρώνοντας αυτές που δεν θέλει .
Δεδομένου τελικά ότι όλο το λογισμικό DRM στηρίζεται στην αληθινή ασφάλεια συσκότισης , βελτιώνει επίσης την ταχύτητα και την ποιότητα απέναντι στις επιθέσεις αυτές.

7.5.3.2 Τα πλεονεκτήματα του DRM

Η ψηφιακή διαχείριση δικαιωμάτων (DRM) είναι μια εύκαμπτη πλατφόρμα η οποία καθιστά ικανή την προστατευμένη και ασφαλή παράδοση και την περιγραφή του περιεχομένου , σε μια αναπαραγωγή ήχου σε έναν υπολογιστή , μια φορητή συσκευή ή μια συσκευή δικτύων . Τα προνόμια που απαιτούν όλοι, οι οποίοι θέλουν να δημιουργήσουν , να παραδώσουν ή να χρησιμοποιήσουν ένα ψηφιακού μέσου περιεχόμενο , είναι να τους παρέχεται η αναγκαία ασφάλεια δεδομένου , να εξασφαλίζεται η ικανοποίηση των χρηστών καθιστώντας διαθέσιμο προς αυτούς περιεχόμενο υψηλής ποιότητας , και τέλος να τους παρέχεται η αναγκαία φορητότητα έτσι ώστε να εξασφαλίζουν ότι θα μπορούν σαν καταναλωτές να απολαύσουν το περιεχόμενο τους οπουδήποτε και αν είναι , με την συσκευή της επιλογής τους .
Η πλατφόρμα της ψηφιακής διαχείρισης δικαιωμάτων (DRM) είναι ικανή για :

- Να βοηθάει τους ιδιοκτήτες να προστατέψουν ικανοποιητικά τα ψηφιακά μέσα τους , το οποίο και ικανοποιείται με το packaging των αρχείων και με τους ισχυρούς αλγόριθμους κρυπτογράφησης .
- Βοηθάει τους ιδιοκτήτες των περιεχομένων , και τις υπηρεσίες των περιεχομένων να πειραματιστούν με νέα επιχειρησιακά μοντέλα μέσω των ιδιοτήτων της πλατφόρμας αυτής .
- Βοηθάει τους καταναλωτές να βρουν , να αποκτήσουν , και να χρησιμοποιήσουν το περιεχόμενο τους ουσιαστικά οπουδήποτε .

7.5.3.3 Τα χαρακτηριστικά γνωρίσματα του Windows Media DRM

Η πιο πρόσφατη έκδοση της ψηφιακής διαχείρισης δικαιωμάτων (DRM) των Windows είναι μια εύκαμπτη πλατφόρμα που το καθιστά πιθανό να προστατεύσει και να παραδώσει ασφαλή την ροή των περιεχομένων , πράγμα που αναλύσαμε και προηγουμένως . Το DRM 10 επιτρέπει συνεχής ροή του περιεχομένου σχεδόν σε οποιαδήποτε συσκευή , ακόμη προσφέρει ένα ευρύ φάσμα επιλογών ενοικίασης των ψηφιακών μέσων , και τέλος διασφαλίζει την ασφάλεια του αρχικού περιεχομένου καθώς αυτό ρέει από συσκευή σε συσκευή .

Ασφαλής παράδοση του περιεχομένου .

Ο Windows Media Right Manager , είναι ένα συστατικό της WMDRM πλατφόρμας, το οποίο βοηθάει στην προστασία των δικαιωμάτων του περιεχομένου των ιδιοκτητών , και το οποίο καθιστά ικανούς τους καταναλωτές να αποκτήσουν το ψηφιακό περιεχόμενο πιο εύκολα και νόμιμα.

- **Επίμονη Προστασία :** Ο Windows Media Right Manager, κλειδώνει τα αρχεία των ψηφιακών μέσων , με ένα κλειδί αδειών για να διατηρήσει έτσι το περιεχόμενο ασφαλισμένο , ακόμη και αν τα αρχεία αυτά είναι ευρέως διανεμημένα .Κάθε άδεια είναι μοναδική και ορίζεται ξεχωριστά σε κάθε υπολογιστή . Αυτό αποτρέπει την παράνομη διανομή των ψηφιακών αρχείων μέσων .

- **Ισχυρή κρυπτογράφηση :** Ο Windows Media Right Manager, περιλαμβάνει τα αποδεδειγμένα σχέδια κρυπτογράφησης που διασφαλίζουν ότι τα διανεμημένα αρχεία μέσων δεν εκτίθενται στην πειρατεία ή σε άλλη παράνομη χρήση .

- **Εξατομίκευση :** Ο Windows Media Right Manager καθιστά κάθε τομέα μοναδικό , με το να συνδέει τον φορέα αυτό με έναν host υπολογιστή .

- **Χωριστά διανεμημένες άδειες και περιεχόμενα :** Οι άδειες εκδίδονται ανεξάρτητα από τα πραγματικά ψηφιακά αρχεία μέσων , παρέχοντας την μέγιστη ευελιξία και επιτρέποντας την ευρεία διανομή του περιεχομένου . Κάθε φορά που αναπαράγεται ένα ψηφιακό αρχείο μέσων ο Windows Media Right Manager ελέγχει για να δει εάν ο καταναλωτικός υπολογιστής έχει μια άδεια . Οι καταναλωτές που δεν έχουν μια έγκυρη άδεια , κατευθύνονται σε μια σελίδα εγγραφής αδειών .

- **Ασφαλές ακουστικό μονοπάτι :** Ο Windows Media Right Manager εξασφαλίζει την προστασία του περιεχομένου στο λειτουργικό σύστημα από τον φορέα στην κάρτα ήχου . Αυτή η ασφαλής σχέση μειώνει την πιθανότητα ότι ένα μη εξουσιοδοτημένο πρόγραμμα θα συλλάβει μια ψηφιακή ροή μέσων μέσα σε έναν υπολογιστή .

- **Βελτιωμένη ανάκληση και ανανεωσιμότητα :** Ο Windows Media Right Manager επιτρέπει στου συμβιβασμένους φορείς να ανακληθούν όταν νέοι φορείς διατίθενται .

- **Εύκολο να μετατραπούν οι όροι των αδειών:** Επειδή οι άδειες των ψηφιακών αρχείων μέσων αποθηκεύονται χωριστά, οι όροι χορήγησης αδειών μπορούν να αλλάξουν στον server χωρίς να υπάρχει ανάγκη να ανακατανεμηθεί ή να ξανά τοποθετηθεί σε πακέτο το ψηφιακό αρχείο μέσων .

- **Πραγματικού χρόνου κρυπτογράφηση του περιεχομένου :** Με τον Windows Media Right Manager έκδοσης 9 και προηγούμενων , το περιεχόμενο των ιδιοκτητών μπορεί να παραδοθεί προστατευμένο , μέσω του Internet . Αυτή η νέα ικανότητα προσφέρει την ταυτόχρονη κωδικοποίηση και κρυπτογράφηση και προστατεύει το περιεχόμενο από την αναρμόδια χρήση .

Αναπαραγωγή ήχου σταθερών υπολογιστών.

Η αναπαραγωγή ήχου του προστατευμένου με Windows Media βασισμένου περιεχομένου , είναι καθιερωμένη , με πάνω από 500 εκατομμύρια εγκατεστημένους ψηφιακούς players ικανούς να

προστατεύσουν το περιεχόμενο . Θα αναφέρουμε εδώ μερικές από τις βελτιώσεις που προσφέρει ο Windows Media DRM 10 στους υπολογιστές .

- **Αλυσιδωτές άδειες :** Επιτρέπει στους φορείς παροχής υπηρεσιών των περιεχομένων , να δημιουργήσουν τις άδειες ¨root ¨ που περιέχουν τις πληροφορίες που προσδιορίζουν εάν ένα αρχείο μπορεί να εκτελεστεί ή όχι , όπως για παράδειγμα η ημερομηνία λήξης , και επίσης μπορούν και δημιουργούν ¨φύλλα ¨ αδειών για το ίδιο το περιεχόμενο . Αυτό είναι χρήσιμο για την περιγραφή των υπηρεσιών , καθώς μόνο η μόνη ¨root¨ άδεια , χρειάζεται προκειμένου να ενημερωθεί κάθε περίοδος ανανέωσης σε αντιδιαστολή με την ανανέωση των εκατοντάδων ή χιλιάδων μεμονωμένων αδειών .

- **Βελτιωμένη απόδοση αποθηκευμένων αδειών :** Ελαχιστοποιεί τις καθυστερήσεις δεδομένου ότι οι καταναλωτές αποκτούν περισσότερες άδειες DRM στους υπολογιστές , επιτρέποντας τον εξαγνισμό των παλαιότερων , παρέχει ακόμη , χρόνο- μετρημένες άδειες και κλίμακες βιβλιοθηκών ψηφιακών μέσων καλά αυξημένες .

- **Συγχρονισμένες λίστες :** Αυτόματα συγχρονίζει τις βασισμένες στην αρίθμηση ή στον χρόνο άδειες στις συσκευές .

Αναπαραγωγή ήχου φορητών συσκευών .

Αυτά τα χαρακτηριστικά γνωρίσματα ισχύουν για συσκευές όπως τα φορητά ακουστικά και τα βίντεο player , οι μετασχηματιστές , και οι κινητές συσκευές με τις ακουστικές και τηλεοπτικές ικανότητες . Οι συσκευές όπως αυτές που προαναφέραμε , μπορούν να αποθηκεύουν και να παίζουν το πίσω ακουστικό και τηλεοπτικό περιεχόμενο από έναν τοπικό σκληρό δίσκο , ή να υποστηρίζουν την αναπαραγωγή βίντεο πάνω σε ένα ιδιωτικό δίκτυο όπως σε ένα σύστημα καλωδίων .

- **Αλυσιδωτές άδειες :** Παρουσιάζει τα ίδια χαρακτηριστικά με αυτά της περίπτωσης των αλυσιδωτών αδειών στην αναπαραγωγή ήχου σε σταθερό υπολογιστή .

- **Δοσολογία :** Επεκτείνει την περιγραφή των επιχειρησιακών προτύπων με την διευκόλυνση της ανώνυμης υποβολής των εκθέσεων των διαδρομών που παίζονται . Αυτό παρέχει την επιχειρησιακή υποδομή που επιτρέπει στην περιγραφή του περιεχομένου για να μεταφερθεί στις φορητές συσκευές .

- **Secure Clock: Παρέχει** την ικανότητα για τις συσκευές να αποκτήσουν και να παίξουν το περιεχόμενο της περιγραφόμενης μουσικής σύμφωνα με τους επιχειρησιακούς κανόνες που συνδέονται με την εκάστοτε άδεια.

- **Άμεση απόκτηση αδειών :** Επιτρέπει στις συσκευές οι οποίες είναι σε θέση να συνδεθούν άμεσα με την υπηρεσία παροχής του περιεχομένου , να αποκτήσουν άμεσα το περιεχόμενο , παρά να πρέπει να συνδεθούν μέσω ενός υπολογιστή .

- **Παράγωγα δικαιώματα :**Επιτρέπει στους ιδιοκτήτες των περιεχομένων να διευκρινίσουν διαφορετικά δικαιώματα για τις συσκευές και τους υπολογιστές .

- **Καινοτομία ενοικίασης ή περιγραφής των προτύπων :** Οι φορείς παροχής υπηρεσιών των περιεχομένων , μπορούν να αλλάξουν τους χρόνους έναρξης αδειών , τους χρόνους διακοπής , καθώς και την διάρκεια τους , για να δημιουργήσουν καινοτομικά επιχειρησιακά πρότυπα . Αυτά τα διαφορετικά πρότυπα αφήνουν τους προμηθευτές των περιεχομένων να βελτιώσουν τους επιχειρησιακούς τους κανόνες και να αφήσουν τους υπόλοιπους καταναλωτές να απολαύσουν τα περιεχόμενα τους σε οποιαδήποτε συσκευή .

Αναπαραγωγή ήχου συσκευών δικτύων .

Αυτά τα χαρακτηριστικά γνωρίσματα ισχύουν για συσκευές όπως ,οι μετασχηματιστές , οι φορείς DVD , και οι ψηφιακοί δέκτες . Αυτή η περιεκτικότητα σε ροή συσκευών από έναν υπολογιστή στο τοπικό δίκτυο . Δεν μπορούν να αποθηκεύσουν το περιεχόμενο , και ο περιεχόμενο παραμένει πλήρως κρυπτογραφημένο μέσω του δικτύου .

- **Εξωτερική προστασία** : Αφήνει το περιεχόμενο του καταναλωτικού προϊόντος , σε μια προστατευμένη μορφή πέρα από τα εγχώρια δίκτυα χωρίς την απαίτηση της τοπικής αποθήκευσης .
- **Κρυπτογράφηση βασικού προτύπου.**
- **Ίδιες ικανότητες ανάκλησης με τα PCs και τις φορητές συσκευές** .
- **Ανίχνευση εγγύτητας για ασφαλή και εξουσιοδοτημένη πρόσβαση** .

7.5.4 SKDs and Versions of Windows Media DRM.

To Windows Media digital rights management (DRM), είναι ένα τέλος-προς-τέλος σύστημα το οποίο προσφέρει στους ιδιοκτήτες των περιεχομένων και στους φορείς παροχής υπηρεσιών , μια εύκαμπτη πλατφόρμα για την ασφαλή διανομή των ψηφιακών αρχείων μέσων , και στους καταναλωτές προσφέρει την ευκολία χρήσης αυτών των μηχανημάτων , πράγμα απαραίτητο για να απολαύσουν την εμπειρία των ψηφιακών μέσων . Η λύση DRM αποτελείται και από τα δύο και από λογισμικό ανάπτυξης του server , αλλά και από λογισμικό ανάπτυξης του client (SKDs) , που επιτρέπουν στις εφαρμογές να προστατευτούν και να αναπαράγουν τα προηγούμενα ψηφιακά αρχεία μέσων .
Ο server SKD είναι χορηγημένος με μία άδεια με την ονομασία Windows Media digital rights management SKD, και ο client SKD είναι και αυτός επίσης χορηγημένος με μια άδεια ως συστατικό του σχήματος Windows Media SKD. Η τελευταία έκδοση του Windows Media DRM περιλαμβάνει νέα χαρακτηριστικά τα οποία παρέχουν γερές ικανότητες για να μπορούν να αποκτήσουν και να έχουν πρόσβαση να προστατεύσουν το περιεχόμενο τους στις φορητές συσκευές και τις συσκευές δικτύων .
Οι παρακάτω πληροφορίες θα μας βοηθήσουν να κατανοήσουμε τις απαιτήσεις μας και να καθορίσουμε ποιες από τις υπάρχουσες τεχνολογίες είναι κατάλληλες για τις ανάγκες μας .

7.5.4.1 Επιλογή της SKD που χρειαζόμαστε .

Χρησιμοποιώντας το Windows Media digital rights management SKD (client SKD),οι υπεύθυνοι μπορούν να δημιουργήσουν ,από την μεριά του πελάτη , εφαρμογές οι οποίες έπαιζαν επαναλαμβανόμενα πακέτα των Windows Media αρχείων . Το SKD Media , δίνει την δυνατότητα στις εφαρμογές αυτές να αποκτούν άδειες , να αποθηκεύει και να ανακτά τις άδειες αυτές και να παρέχει βελτιώσεις σε ζητήματα ασφάλειας για τα συστατικά του DRM.
Οι υπεύθυνοι για την ανάπτυξη λογισμικού μπορούν να χρησιμοποιήσουν τον Windows Media Right Manager , ο οποίος είναι επίσης ένα χαρακτηριστικό γνώρισμα του SKD Media Windows , για να διευκολύνει την μεταφορά των συσκευασμένων αρχείων media Windows από το PC σε μια φορητή συσκευή .
Η πλατφόρμα Media DRM 10 περιλαμβάνει δύο νέες τεχνολογίες , οι οποίες επιτρέπουν την αναπαραγωγή ήχων στις φορητές συσκευές και τις συσκευές δικτύων . Επιπλέον , η εφαρμογή του κώδικα αντικειμένου της Portable Device DRM version1 , είναι ένα χαρακτηριστικό του Windows Media Embedded Product Adaption Kit (PAK).

Πίνακας 10 : Περιγραφή λειτουργιών της πλατφόρμας Media DRM 10.

Λειτουργιά/Υπηρεσία	**Ποιος**	**Ενέργεια**	**Windows Media DRM Τεχνολογίες**
Packaging Περιεχομένου	Ετικέτες, στούντιο και φορείς παροχής υπηρεσιών	Κρυπτογράφηση των συμπιεσμένων ψηφιακών μέσων	Windows Media Rights Manager SKD
Hosting Περιεχομένου	Πωλητές λιανικής και φορείς παροχής υπηρεσιών	Φιλοξένηση και διανομή του ψηφιακού περιεχομένου μέσων	Windows Media server or Web server
License clearing house	Φορείς παροχής υπηρεσιών	Ζητήματα αδειών . Συναλλαγές διαδρομής	Windows Media Rights Manager SKD
Playback Περιεχομένου	Υπεύθυνοι για την ανάπτυξη εφαρμογής	Εκτέλεση του προστατευμένου ψηφιακού μέσου	Windows MediaDRM component in Windows Media Format SKD
Portable Device Playback	Υπεύθυνοι για την ανάπτυξη υλικού	Μεταφορά και εκτέλεση του προστατευμένου ψηφιακού μέσου	Windows Media DRM 10 for Portable Devices,
Network device Playback	Υπεύθυνοι για την ανάπτυξη υλικού	Εκτέλεση του προστατευμένου ψηφιακού μέσου από απομακρυσμένη	Windows Media DRM 10 for Network Devices

		πηγή	

7.5.4.2 Επιλογή της έκδοσης του Windows Media DRM 10 που χρειαζόμαστε .

Η χορήγηση των αδειών της τελευταίας έκδοσης του Windows Media Rights Manager SDK , παρέχει σε μας την δυνατότητα να χρησιμοποιούμε την πιο πρόσφατη τεχνολογία έχοντας οπισθοδρομική συμβατότητα . Ένας Windows Media Rights Manager 10.1 SDK κάτοχος άδειας , είναι σε θέση να διανείμει ,σε όλες τις προηγούμενες και νέες εκδόσεις του Windows Media DRM ,τις άδειες αυτές. Ένας κάτοχος άδειας θα είναι σε θέση να εφαρμόσει τα νεώτερα χαρακτηριστικά γνωρίσματα , συμπεριλαμβανομένης και της απευθείας κρυπτογράφησης και τις ενισχυμένης ασφάλειας .
Η ερώτηση συχνά ξεκινά από τους προμηθευτές των περιεχομένων , σχετικά με το ποια έκδοση DRM άδειας θα προορίζεται για ένα δεδομένο κομμάτι συσκευασμένου περιεχομένου .
Μια παλιά έκδοση άδειας (πχ η version 1) και μια νέα έκδοση άδειας (πχ η πιο πρόσφατη η version 7), διαφέρουν κυρίως από άποψη επιπέδων ασφαλείας , τα οποία μπορούμε να εφαρμόσουμε , καθώς επίσης και ο βαθμός καταναλωτικής προσιτότητας .
Συστήνεται να εξετάζουμε τις ανταλλαγές μεταξύ της προστασίας περιεχομένου και της καταναλωτικής προσιτότητας , και στην συνέχεια να αποφασίζουμε ποια άδεια DRM θέλουμε να εκδώσουμε :

- Εάν επιθυμούμε να συνεχίζουμε να χρησιμοποιούμε την έκδοση 1 του Windows Media DRM , κύριο χαρακτηριστικό μας είναι η προσιτότητα . Εντούτοις δεν θα έχουμε την προστιθέμενη προστασία της καινούργιας ικανότητας και της επιθυμητής ανάκλησης σε περίπτωση που κάποια ευπάθεια ανιχνευτεί .

- Εάν επιθυμούμε αυξημένο επίπεδο ασφάλειας , αλλά και ταυτόχρονη ευρεία καταναλωτική προσιτότητα , μπορούμε να εφαρμόσουμε ,την έκδοση 1 ή την έκδοση 9, για να χορηγήσουμε άδεια για κάθε κομμάτι του περιεχομένου . Παρόλα αυτά , οποιαδήποτε ευπάθεια , που ανιχνεύεται στην έκδοση 1 έχει επιπτώσεις στην ασφάλεια του περιεχομένου .

- Εάν επιθυμούμε το ασφαλέστερο μέτρο , οδηγούμαστε στην επιλογή της έκδοσης 9 του Windows Media αδειών . Δεν θα πραγματοποιήσουμε καθόλου καμία άδεια έκδοσης 1. Αυτό το μέτρο θα απέκλειε τους χρήστες του Windows Media Player , από το να έχουν πρόσβαση στο προστατευμένο περιεχόμενο.

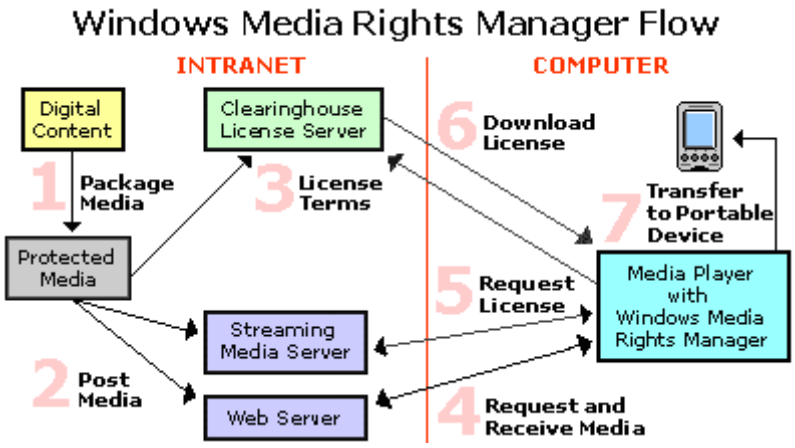
Πίνακας 11 Εκδόσεις του Media DRM .

	Windows Media DRM Version 1	Windows Media DRM Version 7.x and 9	Windows Media DRM Version 10
Έκδοση σχεδίου	Απρίλιος 1999	Ιανουάριος 2003	2004
Λειτουργικά συστήματα	Windows 95, Windows 98, Windows NT 4.0, Windows 2000, Windows Millennium Edition , Windows XP, και στα Mac OS 8.1	Windows 98, Windows 2000, Windows Millennium Edition , και στα Windows XP	Windows XP, Windows Vista.
Υποστήριξη Portable Device	Υποστηρίζει SDMI συσκευές , τις μη-SDMI συσκευές , και φορητές συσκευές.	Υποστηρίζει SDMI συσκευές , τις μη-SDMI συσκευές , και φορητές συσκευές.	Υποστηρίζει φορητούς ακουστικούς player , κινητά τηλέφωνα ,DVD Player κα.
Κώδικες	Windows Media Audio 1,2 και 7, Windows Media Video 7 , Windows MPEG-4 version 1, ACELP,Voxware,ATRAC-3	Windows Media Audio 1,2,7,8,9, 9 Professional , 9 Voice , Windows Media Video 7,8,9 ,9 Image, Windows MPEG-4 version 1, και Windows Media Screen 7	Windows Media Audio 1,2,7,8,9, 9 Professional , 9 Voice , Windows Media Video 7,8,9 ,9 Image, Windows MPEG-4 version 1, και Windows Media Screen 7
Επιχειρηματικού κανόνες	• Ημερομηνία λήξης . • Απεριόριστη χρήση . • Μεταφορά σε SDMI και μη – SDMI συσκευές . • Κάψιμο σε CD	• Ημερομηνία λήξης . • Απεριόριστη χρήση . • Μεταφορά σε SDMI και μη – SDMI συσκευές . • Κάψιμο σε CD. • Χρόνος έναρξης . • Χρόνος λήξης . • Διάρκεια . • Αριθμημένες διαδικασίες .	• Ημερομηνία λήξης. • Απεριόριστη χρήση. • Κάψιμο σε CD. • Χρόνος έναρξης. • Χρόνος λήξης. • Διάρκεια. • Αριθμημένες διαδικασίες.

Εμπειρία του χρήστη	Η αθόρυβη χορήγηση αδειών και η προ-παράδοση των αδειών δεν υποστηρίζονται . Οι χρήστες γνωρίζουν πολύ πρόσθετα βήματα και πρέπει να κατευθυνθούν άμεσα εκεί.	• Αθόρυβη χορήγηση αδειών. • Προ-παράδοση αδειών. • Αποθήκευση και αποκατάσταση αδειών. • Πρότυπα διαλόγων μέσα στα Player . • Διαχείριση αδειών	• Μεγαλύτερη λειτουργία συσκευών. • Περιγραφή περιεχομένου και μεταφορά στις συσκευές . • Ταχύτερη απόκτηση και ανανέωση αδειών . • Playback του προστατευμένου περιεχομένου σε συσκευές δικτύων.
Ασφάλεια	Κρυπτογράφηση του περιεχομένου και της άδειας .	Κρυπτογράφηση του περιεχομένου και της άδειας . Και επιπλέον : • Εξατομίκευση. • Ασφαλές μονοπάτι ήχου • Ανάκληση της εφαρμογής φορέων. • Ανάκληση του περιεχομένου. • Αποκλεισμός της εφαρμογής φορέα. • Αποκλεισμός του Module του προστατευμένου περιεχομένου .	Όμοια με την προηγούμενη έκδοση . Και επιπλέον : • Ανάκληση και ο αποκλεισμός επεκτείνονται και στις φορητές συσκευές και στις συσκευές δικτύου .

7.5.5 Αρχιτεκτονική δομή του Windows Media Rights Manager.

Όταν ένας καταναλωτής αποκτήσει ένα κρυπτογραφημένο ψηφιακό αρχείο μέσων από έναν Ιστοχώρο , πρέπει επίσης να αποκτήσει μια άδεια που περιέχει ένα κλειδί για να ξεκλειδώσει το αρχείο προτού μπορέσει να το χρησιμοποιήσει . Οι ιδιοκτήτες των περιεχομένων μπορούν εύκολα να θέσουν αυτά τα κλειδιά και τις άδειες αυτές , σε κίνηση προστατεύοντας τα αρχεία του περιεχομένου τους , με τον Windows Media Rights Manager , και διανέμοντας στην συνέχεια το περιεχόμενο τους στους καταναλωτές .
Η ακόλουθη απεικόνιση επιδεικνύει πως το περιεχόμενο προστατεύεται , διανέμεται , και χρησιμοποιείται από τον Windows Media Rights Manager.



Εικόνα 115 : Απεικόνιση της αρχιτεκτονικής του Windows Media Rights Manager.

7.5.5.1 Πως λειτουργεί ο Windows Media Rights Manager.

Ο Windows Media Rights Manager επιτρέπει στους προμηθευτές να παραδώσουν τραγούδια , βίντεο , κι άλλο είδος τύπου ψηφιακό περιεχόμενο , και όλα αυτά μέσω του διαδικτύου , με ένα προστατευμένο κρυπτογραφημένο σχήμα αρχείων . Ο Windows Media Rights Manager βοηθάει να προστατευτούν τα ψηφιακά μέσα με το packaging των αρχείων των ψηφιακών μέσων .
Ένα πακεταρισμένο αρχείο μέσων περιέχει μια έκδοση ενός αρχείου μέσων ,που έχει κρυπτογραφηθεί και έχει ασφαλιστεί με ένα κλειδί . Αυτό το συσκευασμένο αρχείο συσσωρεύει επίσης πληροφορίες του ιδιοκτήτη του περιεχομένου . Το αποτέλεσμα όλων είναι ένα συσκευασμένο αρχείο μέσων που μπορεί μόνο να χρησιμοποιηθεί από κάποιο συγκεκριμένο πρόσωπο που έχει λάβει την σωστή άδεια.

Η βασική διαδικασία του Windows Media Rights Manager είναι η ακόλουθη :

- **Packaging**
  Ο Windows Media Rights Manager συσκευάζει τα ψηφιακά αρχεία μέσων .Το πακετάρισμα των αρχείων αυτών γίνεται κρυπτογραφώντας τα και κλειδώνοντας τα με ένα ¨κλειδί¨. Αυτό το κλειδί αποθηκεύεται σε μια κρυπτογραφημένη άδεια , η οποία διανέμεται ξεχωριστά. Και άλλες

πληροφορίες είναι προστιθέμενες στα αρχεία των μέσων , όπως η URL που μπορεί η άδεια να αποκτηθεί. Το πακετάρισμα των ψηφιακών αρχείων μέσων , αποθηκεύεται σε έναν Windows Media Audio τύπο αρχείου (με .wma κατάληξη αρχείου) ή σε Windows Media Video τύπο (με .wmv κατάληξη αρχείου).

- **Διανομή**
  Το πακετάρισμα των αρχείων μπορεί να τοποθετηθεί σε ένα Web site για download , μπορεί να τοποθετηθεί σε έναν media server για streaming , μπορεί να διανεμηθεί σε CD ,ή να αποσταλθεί στους καταναλωτές . Ο Windows Media Rights Manager επιτρέπει στους καταναλωτές να στέλνουν αντίγραφα προστατευμένων ψηφιακών αρχείων μέσων , στους φίλους τους .

- **Καθιέρωση ενός κεντρικού υπολογιστή αδειών**
  Οι προμηθευτές των περιεχομένων επιλέγουν ένα ¨καθαρό¨ μέρος στο οποίο αποθηκεύονται τα συγκεκριμένα δικαιώματα και οι κανόνες των αδειών , και εφαρμόζονται οι υπηρεσίες των αδειών του Windows Media Rights Manager. Ο ρόλος του καθαρού αυτού μέρους είναι να επικυρώνει τις αιτήσεις των καταναλωτών για να τους παράσχει άδεια. Οι άδειες και τα ψηφιακά αρχεία διαμοιράζονται και αποθηκεύονται ξεχωριστά , κάνοντας έτσι ευκολότερη όλη την διαδικασία διαχείρισης του συστήματος .

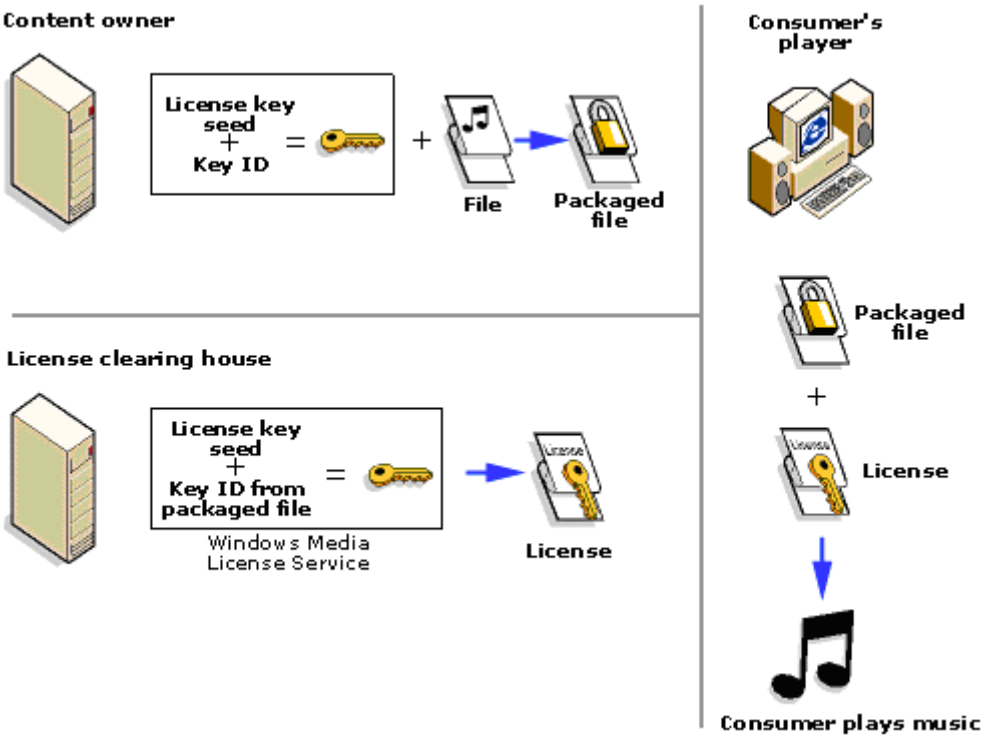
- **Απόκτηση αδειών**
  Προτού χρησιμοποιηθεί ένα packaging ψηφιακό αρχείο μέσων , οι καταναλωτές πρέπει πρώτα να αποκτήσουν το κλειδί της άδειας για να ξεκλειδώσουν το αρχείο αυτό . Η διαδικασία της απόκτησης της άδειας , ξεκινάει αυτόματα όταν ο καταναλωτή προσπαθήσει να αποκτήσει το προστατευμένο περιεχόμενο , αρχικά αποκτά μια προ-παραδομένη άδεια . Ο Windows Media Rights Manager είτε στέλνει τον καταναλωτή σε μια σελίδα εγγραφής ,όπου ζητούνται οι πληροφορίες ή απαιτείται πληρωμή , ή ακόμη αθόρυβα ανακτάται η άδεια .

- **Χρησιμοποίηση των αρχείων μέσων**
  Για να χρησιμοποιήσουμε το αρχείο του ψηφιακού αρχείου μέσων , οι καταναλωτές χρειάζονται ένα media player το οποίο υποστηρίζει τον Windows Media Rights Manager. Οι καταναλωτές μπορούν να χρησιμοποιούν τα αρχεία αυτά με βάση τους κανόνες και τα δικαιώματα που συμπεριλαμβάνονται στις άδειες . Οι άδειες μπορούν να έχουν διαφορετικά δικαιώματα όπως τους χρόνους έναρξης , τις ημερομηνίες , την διάρκεια τους ή ακόμη και τις μετρήσεις των διαδικασιών . Για παράδειγμα , διαφορετικά δικαιώματα ,μπορούν να επιτρέπουν στους καταναλωτές να χρησιμοποιούν τα ψηφιακά αρχεία μέσων , σε ένα συγκεκριμένο υπολογιστή και να αντιγράφει τα αρχεία αυτά σε άλλες φορητές συσκευές . Οι άδειες παρόλα αυτά δεν είναι μεταβιβάσιμες .Εάν ένας καταναλωτής στείλει ένα πακεταρισμένο ψηφιακό αρχείο μέσων σε έναν φίλο , ο φίλος αυτός πρέπει να αποκτήσει την δική του άδεια για να μπορέσει να χρησιμοποιήσει το αρχείο . Αυτός ο τρόπος χορήγησης αδειών , εξασφαλίζει ότι το πακεταρισμένο ψηφιακό αρχείο μέσων , μπορεί να χρησιμοποιηθεί μόνο από τον υπολογιστή που του έχει χορηγηθεί το κλειδί αδειών για το συγκεκριμένο αρχείο .

7.5.5.2 Πως λειτουργεί το ¨κλειδί¨.

Ο ιδιοκτήτης του περιεχομένου κλειδώνει το περιεχόμενο του με ένα ¨κλειδί ¨ , για να δημιουργήσει ένα πακεταρισμένο αρχείο . Προτού να μπορεί ο καταναλωτής να χρησιμοποιήσει

το αρχείο του , η άδεια του καθαρού χώρου δημιουργεί μια άδεια που περιέχει το κλειδί που μπορεί να ξεκλειδώσει το πακεταρισμένο αρχείο και να κατεβάσει την άδεια στον υπολογιστή του καταναλωτή . Το ακόλουθο διάγραμμα δείχνει πώς το κλειδί δημιουργείται και χρησιμοποιείται από τον Windows Media Rights Manager.



Εικόνα 116 : Περιγραφή της λειτουργίας του κλειδιού της άδειας που χρησιμοποιείται από τον Windows Media Rights Manager.

Για να παραχθεί ένα κλειδί , μια άδεια κλειδιού και ένα κλειδί ID απαιτούνται:

- Η άδεια του κλειδιού , είναι μια τιμή την οποία την γνωρίζει μόνο ο ιδιοκτήτης του περιεχομένου , και ο καθαρός χώρος της άδειας.
- Το κλειδί ID , δημιουργείται από τον ιδιοκτήτη του περιεχομένου για κάθε ένα Windows αρχείο μέσων . Αυτή η τιμή συμπεριλαμβάνεται στο πακεταρισμένο αρχείο .

Όταν η άδεια του καθαρού χώρου πρέπει να εκδώσει μια άδεια για ένα πακεταρισμένο αρχείο , ένα κλειδί αναδημιουργείται με την ανάκτηση του κλειδιού ID από το πακεταρισμένο αρχείο . Η Windows Media Licenses Service χρησιμοποιεί την άδεια του κλειδιού και το κλειδί ID από το πακεταρισμένο αρχείο , για να δημιουργήσει το κλειδί . Το κλειδί περιλαμβάνεται στην άδεια που αποστέλλεται στον υπολογιστή του καταναλωτή . Χρησιμοποιώντας το κλειδί που περιλαμβάνεται στην άδεια , ο Player στον υπολογιστή του καταναλωτή μπορεί να ανοίξει και να χρησιμοποιήσει το προστατευμένο αρχείο .

7.5.5.3 Πως λειτουργούν οι άδειες .

Κάθε άδεια περιλαμβάνει το κλειδί για να ξεκλειδωθεί το Windows αρχείο μέσων . Η άδεια περιέχει επίσης τα δικαιώματα , και τους κανόνες που οι κυβερνήσεις χρησιμοποιούν στα ψηφιακά αρχεία μέσων . Ο ιδιοκτήτης του περιεχομένου ρυθμίζει αυτά τα δικαιώματα για να καθορίσει ποιες ενέργειες επιτρέπονται από τον ελάχιστο έλεγχο της αναπαραγωγής του ήχου στις πιο περιορισμένες άδειες .
Αυτές οι άδειες του Windows Media Rights Manager, μπορούν να υποστηρίζουν ένα μεγάλο εύρος από διαφορετικούς κανόνες επιχειρήσεων συμπεριλαμβανομένων :

- Των πόσων φορών ένα αρχείο μπορεί να αναπαραχθεί .
- Σε μηχανές , τα αρχεία μπορούν να εκτελεστούν ή να μεταφερθούν σε αυτές .
- Ποίο επίπεδο ασφαλείας απαιτείται από τον πελάτη για να εκτελέσει το Windows αρχείο μέσων . κα

7.5.6 Windows Media Rights Manager 10 SDK

Στο τελευταίο αυτό κομμάτι θα περιγράψουμε περιληπτικά την λειτουργία καθώς και την κύρια ιδιότητα του Windows Media Rights Manager 10 SDK. Ο Windows Media Rights Manager 10 SDK είναι ένα από τα κύρια χαρακτηριστικά του Windows Media SDK . Άλλα χαρακτηριστικά που περιλαμβάνονται είναι αυτά του Microsoft Windows Media Services SDK , Microsoft Windows Media Encoder SDK , Microsoft Windows Media Format SDK και το Microsoft Windows Media Player SDK.
Αυτό το χαρακτηριστικό δηλαδή ο Windows Media Rights Manager 10 SDK έχει σχεδιαστεί για εφαρμογές οι οποίες επιθυμούν να παραδίδουν ψηφιακά μέσα , όπως για παράδειγμα ένα τραγούδι ένα βίντεο ,μέσω του Internet και μέσω ενός προστατευμένου ασφαλούς τρόπου . Ο Windows Media Rights Manager 10 SDK παρέχει εργαλεία για την προστασία των ψηφιακών αρχείων , έτσι μπορούμε να τα διανείμουμε και να τα διατηρήσουμε την προστασία των πνευματικών τους δικαιωμάτων. Η λύση που παρέχεται με τον Windows Media Rights Manager 10 SDK , είναι αρκετά εύκαμπτη ώστε να μπορεί να προσαρμοστεί εύκολα στο τρέχον επιχειρησιακό πρότυπο .
Ο Windows Media Rights Manager 10 SDK είναι ένα ισχυρό εργαλείο το οποίο παρέχει τα ακόλουθα οφέλη για τα Windows Media αρχεία.

- **Ασφάλεια** , μπορεί να κρυπτογραφεί κάθε αρχείο Windows Media , όπως και απαιτούν τα πρόσθετα επίπεδα ασφάλειας . Για παράδειγμα , μπορούμε να περιορίσουμε το playback των εφαρμογών εκείνων μόνο , που είχαν λάβει την αναβάθμιση ασφάλειας , απαιτώντας ένα κατώτατο επίπεδο ασφάλειας για όλους τους φορείς και τις φορητές συσκευές .
- **Ισχυρά χαρακτηριστικά** , μπορούμε να παράγουμε ένα σύνθετο σύνολο δικαιωμάτων για κάθε αρχείο Windows Media , που κυμαίνεται από τον ελάχιστο έλεγχο της αναπαραγωγής του ήχου έως τους περιορισμούς όπως είναι η μέτρηση των διαδικασιών και η λήξη αυτών . Μπορούμε επίσης να ελέγξουμε πώς να εκδίδουμε τις άδειες και πότε .
- **Εξελιξιμότητα ,** έχουμε μεγάλο έλεγχο πάνω στις ρυθμίσεις του digital rights management συστήματός μας . Εάν έχουμε μια μεγάλη ποσότητα δικτυακών δραστηριοτήτων , μπορούμε εύκολα να διαιρέσουμε σε διάφορους ρόλους τον Windows Media Rights Manager 10 SDK πάνω σε οποιοδήποτε αριθμό κεντρικών υπολογιστών .

8 Βιβλιογραφία .

[1] Windows Vista A, B, C – Δημοσιογραφικός Οργανισμός Λαμπράκη 2006.
[2] http://www.wikipedia.org
[3] http://www.microsoft.com
[4] http://www.technet.microsoft.com
[5] http://www.bitlocker.com
[6] http://www.windowshelp.microsoft.com
[7] http://www.leastprivilege.com
[8] http://www.windowsvistaplace.com
[9] http://www.windowsupdate.com