Περιεχόμενα

Πρόλογος 19

1. ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ 23

1.1. ΕΙΣΑΓΩΓΗ 24
1.1.1. Μια σύντομη περιγραφή 24
1.1.2. Απόψεις στο ηλεκτρονικό έγκλημα 24
1.1.3. Κατηγορίες ηλεκτρονικού εγκλήματος 25
1.1.4. Μια σύντομη ιστορική αναδρομή 27
1.2. ΟΙ «ΓΝΩΣΤΟΙ-ΑΓΝΩΣΤΟΙ» HACKERS 31
1.2.1. Το Προφίλ των hackers 31
1.2.2. Τα διάφορα είδη των hackers 32
1.2.2.1. Εσωτερικοί χρήστες (Insiders) 33
1.2.2.2. Κατάσκοποι (Spies) 34
1.2.2.3. Βάνδαλοι (Vandals) 34
1.2.2.4. Οι «ανένταχτοι» 35
1.3. ΟΙ ΣΤΟΧΟΙ ΤΩΝ HACKERS 37
1.4. ΜΕΘΟΔΟΙ ΑΠΟΚΤΗΣΗΣ ΚΑΙ ΔΙΑΚΙΝΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ 38
1.4.1. Passwords 38
1.4.2. Shoulder surfing 39
1.4.3. Dustbin diving 41
1.4.4. Social engineering (Κοινωνική Μηχανική) 42
1.5. ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ 44
1.5.1. Το Ευρωπαϊκό νομικό πλαίσιο 44
1.5.1.1. Council of Europe Recommendation R(89)9 44
1.5.1.2. Η διεθνής σύμβαση για το ηλεκτρονικό έγκλημα (Convention on Cyber Crime) 47
1.5.2. Το Ελληνικό νομικό πλαίσιο 50
1.5.2.1. Ποινικός κώδικας – Άρθρο 370Α 50
1.5.2.2. Ποινικός κώδικας – Άρθρο 370Γ 53
1.5.2.3. Νόμος 2672/1998, Άρθρο 14 (Διακίνηση εγγράφων με ηλεκτρονικά μέσα) 55
1.5.2.4. Νόμος 2472/1997 (Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα) 56
1.6. COMPUTER FORENSICS 57
1.6.1. Ηλεκτρονικά αποδεικτικά στοιχεία και πειστήρια (electronic evidence) 57
1.6.2. Η επιστήμη των computer forensics 58
1.6.3. Που βρίσκονται οι (ηλεκτρονικές) αποδείξεις 60
1.6.3.1. Στάσιμος χώρος (Slack Space) 61
1.6.3.2. Ελεύθερος χώρος (Free Space) 62

1.6.3.3. Το αρχείο ανταλλαγής (swap file) ... 62
1.6.3.4. Άλλες πιθανές πηγές ανεύρεσης τέτοιων πληροφοριών ... 62
1.6.4. Επιλογή του κατάλληλου εξοπλισμού για computer forensics ... 64
1.6.5. Πώς δημιουργείται ένα κατάλληλο αντίγραφο ενός σκληρού δίσκου ... 66
1.6.6. Συνηθισμένα λάθη στο χειρισμό ηλεκτρονικών αποδεικτικών στοιχείων ... 67
1.6.7. Η αλληλουχία επιτήρησης (chain of custody) των ηλεκτρονικών στοιχείων ... 68

2. ΚΡΥΠΤΟΓΡΑΦΙΑ ... 71
2.1. ΕΙΣΑΓΩΓΗ ... 72
2.2. ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ... 74
2.2.1. Εισαγωγή ... 74
2.2.2. Βασικοί Ορισμοί ... 74
2.2.3. Συμμετρικά και ασύμμετρα κρυπτοσυστήματα ... 77
2.2.4. Κρυπταναλυτικές τεχνικές, επιθέσεις και απειλές ... 78
2.2.5. Αποτίμηση επιπέδου ασφάλειας ενός κρυπτοσυστήματος ... 82
2.2.6. Διαφορές μεταξύ συμμετρικών και ασύμμετρων κρυπτοσυστημάτων ... 84
2.3. ΙΣΤΟΡΙΚΟΙ ΚΡΥΠΤΟΓΡΑΦΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ ... 87
2.3.1. Εισαγωγή ... 87
2.3.2. Ο αλγόριθμος του Καίσαρα ... 87
2.3.3. Αλγόριθμοι Απλής Αντικατάστασης ... 90
2.3.4. Τα στατιστικά της αγγλικής γλώσσας ... 91
2.3.5. Ο αλγόριθμος Playfair ... 93
2.3.6. Ομόφωνοι Κώδικες ... 95
2.3.7. Πολυαλφαβητικοί Κώδικες - Κώδικες Vigenere ... 96
2.3.8. Τα πρώτα συμπεράσματα ... 99
2.3.9. Η απόλυτη μυστικότητα ... 100
2.3.10. Το one-time-pad ... 102
2.3.11. Συμπεράσματα ... 103
2.4. ΜΟΝΤΕΡΝΟΙ ΚΡΥΠΤΟΓΡΑΦΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ ... 106
2.4.1. Εισαγωγή ... 106
2.4.2. Δυαδικές ακολουθίες χαρακτήρων ... 106
2.4.3. Stream Αλγόριθμοι ... 108
2.4.4. Κριτήρια σχεδιασμού κρυπτογραφικών αλγορίθμων ... 111
2.4.5. Block Αλγόριθμοι ... 112
2.4.5.1. Τρόπος ECB (Electronic Codebook) ... 113
2.4.5.2. Ενεργές επιθέσεις και επιθέσεις αλλοίωσης του μηνύματος ... 115
2.4.5.3. Τρόπος CFB (Cipher FeedBack) ... 116
2.4.5.4. Τρόπος CBC (Cipher Block Chaining) ... 118
2.4.6. Σύγκριση stream και block αλγορίθμων – Κριτήρια επιλογής ... 120
2.4.7. Συναρτήσεις Κατακερματισμού (Hash Functions) ... 121
2.4.8. Συστήματα Δημοσίου Κλειδιού ... 122

2.4.8.1. Ο αλγόριθμος RSA ... 125
2.4.8.2. Ελλειπτικές Καμπύλες ... 126
2.5. ΧΡΗΣΕΙΣ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ... 127
2.5.1. Εμπιστευτικότητα δεδομένων ... 127
2.5.1.1. Ο αλγόριθμος DES ... 127
2.5.1.2. Ο αλγόριθμος AES ... 131
2.5.1.3. Ο αλγόριθμος Blowfish ... 132
2.5.1.4. Ο αλγόριθμος IDEA ... 132
2.5.1.5. Ο αλγόριθμος RC4 ... 132
2.5.2. Ακεραιότητα δεδομένων ... 133
2.5.2.1. Κρυπτογραφικά αθροίσματα ελέγχου ... 133
2.5.2.2. Ψηφιακές υπογραφές ... 135
2.5.2.3. Σύγκριση ψηφιακών υπογραφών και MACs ... 140
2.5.2.4. Σύγκριση ψηφιακών και φυσικών υπογραφών ... 141
2.5.2.5. Επιθέσεις στις ψηφιακές υπογραφές – Συμπεράσματα ... 141
2.5.3. Πιστοποίηση ταυτότητας ... 143
2.5.4. Υποδομή δημόσιου κλειδιού ... 145
2.5.4.1. Η διαδικασία της (ψηφιακής) πιστοποίησης ... 146
2.5.4.2. Απαιτήσεις για μια CA ... 148
2.5.4.3. Το πρότυπο X509 v.3 ... 149
2.5.4.4. Συμπεράσματα ... 150
2.6. ΔΙΑΧΕΙΡΙΣΗ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΚΛΕΙΔΙΩΝ ... 152
2.6.1. Εισαγωγή ... 152
2.6.2. Ο κύκλος ζωής των κλειδιών ... 153
2.6.2.1. Δημιουργία των κρυπτογραφικών κλειδιών ... 154
2.6.2.2. Διανομή και Αποθήκευση των κρυπτογραφικών κλειδιών ... 154
2.6.2.3. Χρήση των κρυπτογραφικών κλειδιών ... 158
2.6.2.4. Αλλαγή των κρυπτογραφικών κλειδιών ... 158
2.6.2.5. Καταστροφή των κρυπτογραφικών κλειδιών ... 159
2.6.3. Επίλογος ... 160

3. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ ... 163
3.1. ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ ΔΙΚΤΥΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ... 164
3.1.1. Πρωτόκολλα Διαδικτύου ... 164
3.1.1.1. Επίπεδο Εφαρμογής ... 165
3.1.1.2. Επίπεδο Μεταφοράς ... 166
3.1.1.3. Επίπεδο Διαδικτύου ... 167
3.1.1.4. Επίπεδο Διασύνδεσης Δικτύου ... 168
3.1.1.5. Φυσικό Δίκτυο ... 169
3.1.2. Διασύνδεση δικτύων υπολογιστών ... 170
3.1.3. Δρομολόγηση ... 170
3.1.4. Ιεραρχία Πρωτοκόλλων ... 172
3.1.5. Σχεδιασμός και αλληλεπίδραση επιπέδων ... 172
3.1.6. Ιδεατή και πραγματική επικοινωνία ... 173
3.1.7. Το μοντέλο αναφοράς OSI ... 173

3.1.7.1.	Επίπεδο 7 (Επίπεδο Εφαρμογής – Application Layer)	174
3.1.7.2.	Επίπεδο 6 (Επίπεδο Παρουσίασης – Presentation Layer)	174
3.1.7.3.	Επίπεδο 5 (Επίπεδο Συνόδου – Session Layer)	175
3.1.7.4.	Επίπεδο 4 (Επίπεδο Μεταφοράς – Transport Layer)	175
3.1.7.5.	Επίπεδο 3 (Επίπεδο Δικτύου – Network Layer)	175
3.1.7.6.	Επίπεδο 2 (Επίπεδο Σύνδεσης Δεδομένων – Data Link Layer)	175
3.1.7.7.	Επίπεδο 1 (Φυσικό Επίπεδο – Physical Layer)	176
3.1.8.	Υπηρεσίες και πρωτόκολλα του Μοντέλου OSI	176
3.1.8.1.	Πρόσβαση στις υπηρεσίες	177
3.1.8.2.	Μονάδες Δεδομένων	177
3.1.8.3.	Συνδέσεις	177
3.1.8.4.	Θέματα αξιοπιστίας	177
3.1.9.	Προτυποποίηση Δικτύων	178
3.1.9.1.	Ο διεθνής Οργανισμός Προτυποποίησης ISO	178
3.1.9.2.	Παραδείγματα Προτύπων Δικτύων	179
3.2.	ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ– ΤΟ ΠΡΟΤΥΠΟ ISO 7498-2	180
3.2.1.	Εισαγωγή	180
3.2.2.	Πεδία ασφάλειας και πολιτικές	181
3.2.3.	Απειλές Ασφάλειας	182
3.2.3.1.	Θεμελιώδεις απειλές	183
3.2.4.	Υπηρεσίες Ασφάλειας	183
3.2.4.1.	Πιστοποίηση Ταυτότητας	183
3.2.4.2.	Έλεγχος πρόσβασης	184
3.2.4.3.	Εμπιστευτικότητα Δεδομένων	184
3.2.4.4.	Μη-αποποίηση	184
3.2.5.	Μηχανισμοί Ασφάλειας	185
3.2.5.1.	Συγκεκριμένοι μηχανισμοί ασφάλειας	185
3.2.5.2.	Γενικοί μηχανισμοί ασφάλειας	187
3.2.6.	Σχέση των υπηρεσιών ασφάλειας με τους μηχανισμούς	189
3.2.6.1.	Σχέση των υπηρεσιών με τα επίπεδα	189
3.2.7.	Διαχείριση Ασφάλειας	192
3.2.7.1.	Κατηγορίες της διαχείρισης ασφάλειας	192
3.3.	ΕΠΙΣΚΟΠΗΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΕΤΑΙΡΙΚΩΝ ΔΙΚΤΥΩΝ	194
3.3.1.	Τεχνολογία Ethernet	194
3.3.2.	Διευθυνσιοδότηση στο Ethernet	195
3.3.3.	Διευθυνσιοδότηση στο Επίπεδο 3 (IP)	195
3.3.4.	Διευθυνσιοδότηση στο Επίπεδο 4 (TCP)	196
3.3.5.	Δίκτυα Τοπικής Περιοχής	199
3.3.5.1.	Το «Λεπτό» Ethernet	199
3.3.5.2.	Σύνδεση με χρήση UTP καλωδίων και hubs	200
3.3.5.3.	Network Sniffers	201
3.3.5.4.	Διακόπτες (switches)	203
3.3.5.5.	IP Δρομολογητές	205
3.3.5.6.	Ιδεατά LAN	206

3.3.5.7. Εγκατάσταση μιας TCP σύνδεσης ... 207
3.3.5.8. Επίθεση Άρνησης εξυπηρέτησης TCP ... 207
3.3.5.9. Επίθεση εξαπάτησης TCP/IP (TCP/IP spoofing) και RDoS ... 208
3.3.6. Ασύρματο LAN (Wireless LAN) ... 208
3.3.7. Δίκτυα στο φυσικό επίπεδο κτιρίου ... 209
3.3.7.1. Η Ραχοκοκαλιά ενός δικτύου (network backbone) ... 209
3.3.7.2. Διασυνδέσεις στο backbone ... 209
3.3.7.3. Διαχείριση δικτύου ... 210
3.3.7.4. Αντιμετώπιση σφαλμάτων ... 210
3.3.7.5. Προσθήκη Firewall ... 211
3.3.7.6. Περαιτέρω σκέψεις ... 211
3.3.8. Δίκτυα Μητροπολιτικής Περιοχής ... 212
3.3.9. Δίκτυα Ευρείας Περιοχής ... 213
3.3.10. Ασφάλεια Μέσων μετάδοσης ... 214
3.3.11. Φυσικός Διαχωρισμός Δικτύων ... 214
3.3.12. Εμπιστευτικότητα Δεδομένων ... 214
3.3. ΑΣΦΑΛΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ – ΤΟ ΠΡΩΤΟΚΟΛΛΟ SNMP ... 215
3.4.1. Εισαγωγή ... 215
3.4.2. Ασφάλεια Διαχείρισης ... 215
3.4.3. Αρχιτεκτονικό μοντέλο ... 217
3.4.3.1. Λειτουργίες του SNMP ... 217
3.4.3.2. Οι μονάδες δεδομένων του πρωτοκόλλου SNMP ... 218
3.4.3.3. Η δομή ενός SNMP μηνύματος ... 218
3.4.3.4. Παραδείγματα Παγίδων ... 219
3.4.4. Βασικοί μηχανισμοί ασφάλειας του SNMPv1 ... 219
3.4.4.1. Μηχανισμός πιστοποίησης ταυτότητας στο SNMPv1 ... 220
3.4.4.2. Αδυναμία κλειδιού του SNMPv1 ... 220
3.4.4.3. Απειλές ασφάλειας ... 220
3.4.5. Υπηρεσίες ασφάλειας στο SNMPv3 ... 220
3.4.5.1. Μοντέλο ασφάλειας του SNMPv3 ... 221
3.4.5.2. Διαχείριση της ασφάλειας του SNMPv3 ... 222
3.5. ΑΣΥΡΜΑΤΑ LANS (WIRELESS LANS) ... 223
3.5.1. Εισαγωγή – Η τεχνολογία ασύρματων LAN ... 223
3.5.2. Συστατικά στοιχεία ενός 802.11 δικτύου ... 223
3.5.3. Καταστάσεις λειτουργίας του 802.11 ... 224
3.5.4. Φυσικό επίπεδο στο 802.11 ... 225
3.5.5. Επίπεδο συνδέσμου δεδομένων 802.11 ... 226
3.5.6. Το πρόβλημα του κρυμμένου σταθμού ... 227
3.5.7. Σύνδεση σε ένα BSS (Basic Service Set) ... 227
3.5.8. Πιστοποίηση ταυτότητας σε ένα ανοικτό σύστημα ... 228
3.5.9. Κλείδωμα MAC διευθύνσεων ... 228
3.5.10. Ο κίνδυνος υποκλοπής ... 228
3.5.11. Περαιτέρω θέματα ... 231
3.5.12. Υπηρεσίες Ασφάλειας στο 802.11b ... 231

3.5.12.1. WEP ... 231
3.5.12.2. Ο αλγόριθμος RC4 ... 232
3.5.12.3. Η λειτουργία του WEP – Φάση 1η: Κρυπτογράφηση και αποστολή ... 232
3.5.12.4. Η λειτουργία του WEP – Φάση 2η: Λήψη και αποκρυπτογράφηση ... 233
3.5.12.5. Πιστοποίηση ταυτότητας μέσω ενός «διαμοιραζόμενου κλειδιού» ... 233
3.5.12.6. Ασφάλεια του WEP ... 233
3.5.12.7. Παθητική επίθεση στο WEP ... 234
3.5.12.8. Ενεργός Επίθεση στο WEP ... 234
3.5.12.9. Εργαλεία Επίθεσης ... 236
3.5.13. Μέτρα προστασίας ενός ασύρματου δικτύου ... 236
3.5.14. Εκδόσεις του 802.11 ... 238
3.6. Η ΤΕΧΝΟΛΟΓΙΑ BLUETOOTH ... 239
3.6.1. Το όραμα της τεχνολογίας Bluetooth ... 240
3.6.2. Piconets and Scatternets ... 240
3.6.3. Ραδιο-Αρχιτεκτονική ... 241
3.6.4. Καταστάσεις σύνδεσης ... 242
3.6.5. Καταστάσεις ασφάλειας του Bluetooth ... 242
3.6.6. Υπηρεσίες επιπέδου σύνδεσης ... 243
3.6.7. Κλειδιά σύνδεσης ... 243
3.6.7.1. Σύνδεση δύο συσκευών ... 244
3.6.7.2. Κλειδί συνδυασμού ... 244
3.6.7.3. Κλειδί κρυπτογράφησης ... 244
3.6.7.4. PIN στο Bluetooth ... 244
3.6.7.5. Επαναχρησιμοποίηση του κλειδιού μονάδος ... 245
3.6.8. Περαιτέρω θέματα ασφάλειας ... 245
3.6.9. Μέτρα ασφάλειας στο Bluetooth ... 246
3.6.10. 802.11 και Bluetooth ... 246
3.7. ΑΣΦΑΛΕΙΑ GSM ... 247
3.7.1. Εισαγωγή ... 247
3.7.2. Αρχιτεκτονική δικτύου Ραδιοκυψελών ... 247
3.7.2.1. Διαχείριση τοποθεσίας της κινητής συσκευής ... 248
3.7.2.2. Πραγματοποίηση κλήσεων ... 248
3.7.3. Η εξέλιξη των κινητών τηλεπικοινωνιών ... 249
3.7.4. Ιστορία της ασφάλειας των κινητών τηλεπικοινωνιών ... 249
3.7.5. GSM (Global System for Mobile Communications) ... 250
3.7.5.1. Στατιστικά χρήσης του GSM ... 250
3.7.5.2. Χαρακτηριστικά του GSM ... 251
3.7.6. Υπηρεσίες του GSM ... 251
3.7.7. Αρχές ασφάλειας στο GSM ... 252
3.7.7.1. Στοιχείο Ταυτότητας Χρήστη (Subscriber Identity Module – SIM) ... 253
3.7.7.2. Αρχές πιστοποίησης ταυτότητας στο GSM ... 253

3.7.7.3. Ο αλγόριθμος πιστοποίησης ταυτότητας του GSM ... 255
3.7.7.4. Κρυπτογράφηση στο GSM ... 255
3.7.7.5. Επίπεδο ασφάλειας της κρυπτογραφίας στο GSM ... 256
3.7.7.6. Αλγόριθμοι κρυπτογράφησης του GSM ... 256
3.7.7.7. Αλγόριθμοι κρυπτογράφησης στο GPRS ... 256
3.7.7.8. Εμπιστευτικότητα της ταυτότητας χρήστη στο GSM ... 257
3.7.8. Αποτελεσματικότητα των χαρακτηριστικών ασφάλειας του GSM ... 257
3.7.9. Περιορισμοί της ασφάλειας του GSM ... 258
3.8. ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑΣ ... 259
3.8.1. Εισαγωγή ... 259
3.8.2. Οι οντότητες που συμμετέχουν σε ένα πρωτόκολλο ασφάλειας ... 259
3.8.3. Πιστοποίηση ταυτότητας ... 261
3.8.4. Ορισμοί ... 261
3.8.4.1. Ασθενής πιστοποίηση ταυτότητας (weak authentication) ... 262
3.8.4.2. Δυνατή πιστοποίηση ταυτότητας (strong authentication) ... 262
3.8.4.3. Κρυπτογραφημένη μονόδρομη πιστοποίηση ταυτότητας ... 262
3.8.5. Φρεσκάδα και ζωντάνια (freshness and liveness) ... 264
3.8.5.1. Nonces ... 264
3.8.5.2. Χρονοσφραγίδες ... 264
3.8.6. Πιστοποίηση ταυτότητας οντότητας βασισμένη σε ψηφιακές υπογραφές ... 265
3.8.7. Πρωτόκολλα ψηφιακών υπογραφών ... 266
3.8.8. Χρήση ψηφιακών πιστοποιητικών ... 266
3.8.9. Εφαρμογές ... 266
3.8.9.1. ISO/IEC 9798 ... 267
3.8.9.2. Εγκατάσταση του DHKE ... 267
3.8.9.3. Χρήση του DHKE ... 268
3.8.9.4. Πρωτόκολλο από-σταθμό-σε-σταθμό (Station-to-Station) ... 269
3.8.9.5. Πρωτόκολλο Needham-Schroeder ... 270
3.8.10. Το πρωτόκολλο Kerberos ... 273
3.8.10.1. Οι οντότητες του πρωτοκόλλου ... 273
3.8.10.2. Το κίνητρο κατασκευής του Kerberos ... 274
3.8.10.3. Ο αλγόριθμος του πρωτοκόλλου (απλή μορφή) ... 275
3.8.10.4. Θέματα ασφάλειας στο Kerberos ... 277
3.8.10.5. Kerberos και Microsoft Windows 2000 ... 277
3.9. SECURE SOCKETS LAYER (SSL) ... 278
3.9.1. Εισαγωγή ... 278
3.9.2. Αρχιτεκτονική του SSL ... 279
3.9.3. Πρωτόκολλα του SSL ... 281
3.9.3.1. Πρωτόκολλο εγγραφής του SSL ... 281
3.9.3.2. Πρωτόκολλο προδιαγραφών κρυπτογραφίας ... 282
3.9.3.3. Πρωτόκολλο συναγερμού ... 282
3.9.3.4. Πρωτόκολλο χειραψίας ... 283

3.9.4. Συμπεράσματα ... 284
3.10. ΤΟ ΠΡΩΤΟΚΟΛΛΟ IPSEC ... 285
3.10.1. Εισαγωγή ... 285
3.10.2. Δομή και υπηρεσίες του IPSec ... 285
3.10.3. Καταστάσεις λειτουργίας του IPSec ... 286
3.10.4. Σχέσεις ασφάλειας (Security Association – SA) ... 288
3.10.5. Πιστοποίηση ταυτότητας και ανταλλαγή κλειδιών ... 289
3.10.6. IKE SA ... 289
3.10.7. Στόχοι ασφάλειας του IKE ... 290
3.11. ΙΔΕΑΤΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ (VIRTUAL PRIVATE NETWORKS) ... 291
3.11.1. Εισαγωγή ... 291
3.11.2. Η ανάγκη για VPNs ... 292
3.11.3. Πώς λειτουργούν τα VPNs ... 293
3.11.4. Αρχιτεκτονικές απομακρυσμένης πρόσβασης με χρήση VPN ... 294
3.11.5. Τεχνολογία VPN ... 295
3.11.6. Πρωτόκολλα VPN ... 296
3.11.7. Το πρωτόκολλο PPTP (Point-to-Point Tunneling Protocol) ... 297
3.11.7.1. Λειτουργία του πρωτοκόλλου ... 297
3.11.8. Η τεχνική L2F (Layer 2 Forwarding) ... 298
3.11.9. Το πρωτόκολλο L2TP (Layer 2 Transfer Protocol) ... 290
3.11.9.1. Πώς λειτουργεί το L2TP ... 290
3.11.9.2. Προτερήματα του L2TP ... 300
3.12. ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ (E-MAIL) ... 300
3.12.1. Εισαγωγή ... 300
3.12.2. Αρχές λειτουργίας του ηλεκτρονικού ταχυδρομείου ... 301
3.12.3. Multi-purpose Internet Mail Extension – MIME ... 302
3.12.4. Θέματα ασφάλειας του e-mail ... 303
3.12.5. Βασική ασφάλεια του e-mail ... 304
3.12.6. E-mail εκτός εταιρικού δικτύου (Internet E-mail) ... 304
3.12.7. Αυξημένη ασφάλεια του e-mail (κρυπτογραφία) ... 305
3.12.8. Πρότυπα ασφάλειας και κρυπτογράφησης των e-mail ... 306
3.12.8.1. Συνημμένα Ασφάλειας (Security attachments) ... 306
3.12.8.2. Ιστορία του S/MIME ... 307
3.12.9. Πρότυπα Κρυπτογραφίας Δημοσίου Κλειδιού (Public-Key Cryptography Standards – KCS#7) ... 307
3.12.9.1. Σύνταξη Κρυπτογραφημένου Μηνύματος (Cryptographic Message Syntax – CMS) ... 308
3.12.9.2. Το PGP (Pretty Good Privacy) ... 309
3.12.9.3. Διαχείριση κλειδιών από το PGP και το S/MIME ... 310
3.12.9.4. Διαχείριση κλειδιών στο PGP ... 313
3.12.9.5. Πέρα από το PGP και το S/MIME ... 314
3.12.10. Έλεγχος ιών και φιλτράρισμα περιεχομένου ... 314

3.12.10. Ασφαλής ρύθμιση του λειτουργικού συστήματος και διαχείριση της εφαρμογής του εξυπηρετητή ηλεκτρονικού ταχυδρομείου ... 315
3.13. ΕΠΙΘΕΣΗ ΚΑΙ ΑΜΥΝΑ ΣΤΟ INTERNET ... 316
3.13.1. Εισαγωγή ... 316
3.13.2. Προκαταρκτική μελέτη & επιλογή στόχου ... 316
3.13.3. Επιλογή ενός εσωτερικού συστήματος-στόχου ... 318
3.13.4. Επιλογή του κατάλληλου εργαλείου ... 319
3.13.5. Εκτέλεση επίθεσης ... 320
3.13.6. Κατοχύρωση και διατήρηση του ελέγχου στο σύστημα ... 321
3.13.7. Αναγνώριση δικτύου-στόχου ... 323
3.13.8. Αναθεώρηση πλάνων ... 324
3.13.9. Συμπεράσματα ... 325
3.13.10. Τεχνολογίες firewall ... 325
3.13.11. Τύποι firewalls ... 326
3.13.11.1. Firewall φιλτραρίσματος πακέτων ... 326
3.13.11.2. Firewall εξέτασης κατάστασης ... 327
3.13.11.3. Firewall κυκλώματος ... 327
3.13.11.4. Firewall επιπέδου εφαρμογής (application – level gateway) ... 328
3.13.12. Αδυναμίες των firewalls ... 330
3.13.13. Συμπεράσματα ... 331
3.13. ΣΥΣΤΗΜΑΤΑ ΑΝΙΧΝΕΥΣΗΣ ΕΙΣΒΟΛΗΣ (INTRUSION DETECTION SYSTEMS) ... 332
3.14.1. Εισαγωγή ... 332
3.14.2. Η εξέλιξη των IDS ... 333
3.14.3. Εσωτερική αρχιτεκτονική των IDS ... 333
3.14.4. Κατηγοριοποίηση των IDS ... 335
3.14.5. Ανάλυση των τεχνολογιών των IDS ... 336
3.14.5.1. IDS Δικτύου (Network Based IDS – NIDS) ... 336
3.14.5.2. Προτερήματα των IDS Δικτύου ... 337
3.14.5.3. Μειονεκτήματα των IDS Δικτύου ... 338
3.14.6. IDS μεμονωμένου συστήματος ... 339
3.14.6.1. Προτερήματα των IDS μεμονωμένου συστήματος ... 339
3.14.6.2. Μειονεκτήματα των IDS Μεμονωμένου συστήματος ... 341
3.14.7. Η ανάγκη για μια συνδυασμένη λύση ... 341
3.14.7.1. Προτερήματα της συνδυασμένης λύσης ... 342
3.14.7.2. Μειονεκτήματα της συνδυασμένης λύσης ... 343
3.14.8. Τι δεν μπορούν να κάνουν τα IDS ... 343
3.14.9. Ανίχνευση παρουσίας ενός IDS και επίθεση ... 344
3.14.9.1. Ανίχνευση IDS ... 345
3.14.9.2. Επίθεση σε IDS ... 346
3.14.10. Αντί επιλόγου ... 349

4. ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ... 351
4.1. ΕΙΣΑΓΩΓΗ ... 352

4.1.1.	Αρχές ασφάλειας υπολογιστικών συστημάτων	352
4.1.2.	Το θεμελιώδες δίλημμα-πρόβλημα	353
4.1.3.	Θεμελιώδεις σχεδιαστικές αρχές ασφάλειας	354
4.1.4.	Η κλίμακα «ανθρώπου – μηχανής»	356
4.1.5.	Δεδομένα ή πληροφορίες;	357
4.2.	ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ	359
4.2.1.	Γενικό μοντέλο ελέγχου πρόσβασης	359
4.2.2.	Διαδικασίες πρόσβασης	360
4.2.3.	Ιδιοκτησία	362
4.2.4.	Δομές ελέγχου πρόσβασης	363
4.2.4.1.	Μήτρα ελέγχου πρόσβασης (Access Cntrol Matrix – ACM)	363
4.2.4.2.	Δυνατότητες (Capabilities)	364
4.2.4.3.	Λίστες Ελέγχου Πρόσβασης (Access Control Lists – ACLs)	365
4.2.4.4.	Ενδιάμεσα συστήματα ελέγχου	365
4.2.4.5.	Δακτύλιοι προστασίας	367
4.2.4.6.	Μερική διευθέτηση (partial ordering)	368
4.2.4.7.	Πλέγματα (Lattices)	369
4.2.4.8.	Ασφάλεια πολλαπλών επιπέδων	371
4.3.	ΜΟΝΤΕΛΑ ΚΑΙ ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ	373
4.3.1.	Γιατί να χρησιμοποιήσουμε τα μοντέλα ασφάλειας	374
4.3.2.	Μοντέλα καταστάσεων μηχανής (automata)	374
4.3.3.	Βασικό θεώρημα ασφάλειας	374
4.4.	ΜΟΝΤΕΛΟ BELL-LAPADULA (BLP)	375
4.4.1.	Πολιτικές του BLP	375
4.4.1.1.	Ιδιότητα-ss (ss-Property)	376
4.4.1.2.	*-Ιδιότητα (*-Property)	376
4.4.1.3.	Ιδιότητα διακριτικής ασφάλειας (Discretionary Security Property ή ds-Property)	377
4.4.2.	Σταθερότητα (Tranquility)	377
4.4.3.	Κρυφά κανάλια	377
4.4.4.	Προτερήματα και περιορισμοί του BLP	378
4.5.	ΜΟΝΤΕΛΟ HARRISON-RUZO-ULLMAN (HRU)	379
4.5.1.	Στοιχειώδεις λειτουργίες και διαρροή δικαιωμάτων πρόσβασης	379
4.5.2.	Ιδιότητες Ασφάλειας του μοντέλου	380
4.6.	ΜΟΝΤΕΛΟ ΤΟΥ ΚΙΝΕΖΙΚΟΥ ΤΟΙΧΟΥ	381
4.6.1.	Στοιχεία του μοντέλου	382
4.6.2.	Ιδιότητες ασφάλειας του μοντέλου	382
4.6.2.1.	Συνοχή (consistency)	383
4.6.2.2.	Ιδιότητα απλής ασφάλειας (Simple Security Property ή ss-Property)	383
4.6.2.3.	*-Ιδιότητα (*-Property)	383
4.7.	ΜΟΝΤΕΛΟ CLARK-WILSON	383
4.7.1.	Έλεγχος πρόσβασης στο μοντέλο Clark-Wilson	384
4.7.2.	Κανόνες πιστοποίησης του μοντέλου	385
4.7.3.	Κανόνες επιβολής του μοντέλου	385

4.8. ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ... 386
4.8.1. Θεμελιώδεις ορισμοί ... 387
4.8.2. Ακεραιότητα του λειτουργικού συστήματος ... 387
4.8.2.1. Καταστάσεις λειτουργίας ... 388
4.8.2.2. Ελεγχόμενη χρήση ... 389
4.8.3. Μηχανισμοί ασφάλειας στον πυρήνα ... 389
4.8.4. Αρχιτεκτονική υπολογιστών ... 389
4.8.4.1. Κύρια μέρη ενός επεξεργαστή (CPU) ... 390
4.8.4.2. Διεργασίες (processes) και νήματα (threads) ... 390
4.8.4.3. Σωρός συστήματος (system stack) ... 391
4.8.4.4. Τύποι μνήμης ... 391
4.8.4.5. Παγίδες και διακοπές (traps & interrupts) ... 392
4.8.5. Μηχανισμοί ασφάλειας στο λειτουργικό σύστημα ... 395
4.8.5.1. Τεμάχια και σελίδες (segments and pages) ... 396
4.8.5.2. Προστασία μνήμης ... 397
4.8.6. Λογική προστασία στο επίπεδο εφαρμογής ... 398
4.9. ΑΣΦΑΛΕΙΑ ΤΩΝ WINDOWS 2000 ... 399
4.9.1. Οντότητες και αρχές ασφάλειας (principals and authorities) ... 400
4.9.2. Πεδία (Domains) ... 401
4.9.3. Προνόμια (privileges) ... 402
4.9.4. Υποκείμενα στα Windows 2000 ... 402
4.9.5. Αντικείμενα στα Windows 2000 ... 403
4.9.6. Δικαιώματα πρόσβασης (Permissions) ... 404
4.9.7. Έλεγχος πρόσβασης ... 405
4.9.7.1. Λίστες ελέγχου πρόσβασης ... 406
4.9.7.2. Κληρονομικότητα ... 407
4.9.8. Διαχείριση Ασφάλειας ... 408
4.9.9. Συμπεράσματα ... 409

5. ΕΙΔΙΚΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ... 401
5.1. ΒΙΟΜΕΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ ... 412
5.1.1. Εισαγωγή ... 412
5.1.2. Βιομετρικά συστήματα και μέθοδοι πιστοποίησης ταυτότητας ... 412
5.1.3. Βιομετρικά χαρακτηριστικά ... 413
5.1.4. Αρχιτεκτονική βιομετρικών συστημάτων ... 414
5.1.4.1. Διαδικασία εγγραφής του χρήστη στο σύστημα ... 415
5.1.4.2. Υποσύστημα απόκτησης των βιολογικών δεδομένων (data acquisition module) ... 415
5.1.4.3. Υποσύστημα εξαγωγής του χαρακτηριστικού (feature extraction module) ... 415
5.1.4.4. Υποσύστημα σύγκρισης (matching module) ... 416
5.1.4.5. Υποσύστημα απόφασης (decision module) ... 416
5.1.4.6. Υποσύστημα αποθήκευσης (storage module) ... 416
5.1.5. Σφάλματα στις βιομετρικές συσκευές ... 417
5.1.6. Αποτίμηση επιδόσεων ... 417

5.1.7.	Βιομετρικές τεχνολογίες	417
5.1.7.1.	Αναγνώριση υπογραφής	418
5.1.7.2.	Αναγνώριση φωνής	419
5.1.7.3.	Αναγνώριση δακτυλικού αποτυπώματος	420
5.1.7.4.	Πιστοποίηση αποτυπώματος	421
5.1.7.5.	Εξέταση οφθαλμικού αμφιβληστροειδούς χιτώνα	421
5.1.7.6.	Εξέταση ίριδας ματιού	422
5.1.7.7.	Αναγνώριση προσώπου	423
5.1.7.8.	Γεωμετρία παλάμης	424
5.1.7.9.	Άλλες βιομετρικές μέθοδοι	424
5.2.	ΧΕΙΡΙΣΜΟΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ	425
5.2.1.	Η Διοικητική Πλευρά - Εμπλεκόμενα μέλη	427
5.2.2.	Δημιουργία Ομάδας Αντιμετώπισης Περιστατικών Ασφάλειας	430
5.2.3.	Η Τεχνική Πλευρά - Μεθοδολογία Αντιμετώπισης Περιστατικών Ασφάλειας	433
5.2.3.1.	Προετοιμασία (Preparation)	433
5.2.3.2.	Αναγνώριση (Identification)	434
5.2.3.3.	Περιορισμός (Containment)	434
5.2.3.4.	Εξάλειψη (Eradication)	435
5.2.3.5.	Ανάκαμψη (Recovery)	435
5.2.3.6.	Επακόλουθα(Followup)	435
5.3.	ΥΠΟΔΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΟ ΕΜΠΟΡΙΟ – ΜΥΘΟΙ ΚΑΙ ΠΡΑΓΜΑΤΙΚΟΤΗΤΑ	436
5.3.1.	Κρυπτογραφία Δημόσιου Κλειδιού	436
5.3.1.1.	Εισαγωγή	436
5.3.1.2.	Ψηφιακά Πιστοποιητικά και Υποδομή Δημόσιου Κλειδιού	437
5.3.2.	Κρυπτογραφία και ηλεκτρονικό εμπόριο	440
5.3.3.	Κρυπτογραφία και Ανωνυμία	441
5.3.4.	Εμπιστοσύνη και Πιστοποίηση Ταυτότητας στις Ηλεκτρον. Συναλλαγές	442
5.3.4.1.	Διεθνείς Συναλλαγές με χρήση πιστωτικών καρτών	442
5.3.4.2.	Ηλεκτρονικές Συναλλαγές με τη Χρήση Ψηφιακών Πιστοποιητικών	444
5.3.5.	Η σημερινή πραγματικότητα	451
5.3.6.	Συμπεράσματα	453
5.4.	ΙΟΜΟΡΦΙΚΟ ΛΟΓΙΣΜΙΚΟ	455
5.4.1.	Εισαγωγή	455
5.4.2.	Δομή ιών	455
5.4.2.1.	Ιοί τομέα εκκίνησης (Boot Record Viruses)	456
5.4.2.2.	Προγραμματιστικοί/Παρασιτικοί ιοί (Parasitic Viruses)	458
5.4.2.3.	Κρυφοί ιοί (Stealth Viruses)	459
5.4.2.4.	Κρυπτογραφημένοι ιοί	460
5.4.2.5.	Πολυμορφικοί ιοί (Polymorphic Viruses)	461
5.4.2.6.	Ιοί Ρετρό (Retro Viruses)	462

5.4.2.7. Ιοί συνδέσμων (Link Viruses) ... 462
5.4.2.8. Πολύ-διαχωρισμένοι Ιοί (Multipartite Viruses) ... 462
5.4.2.9. Macro Ιοί ... 463
5.4.3. Άλλες μορφές «κακού κώδικα» (malicious code) ... 464
5.4.3.1. Σκουλήκια (Worms) ... 464
5.4.3.2. Λογικές βόμβες ... 465
5.4.4. Πόσο εύκολα δημιουργείται ένας ιός ... 465
5.4.5. Το μέλλον ... 466

Α. ΠΑΡΑΡΤΗΜΑ - ΤΟ ΠΡΌΓΡΑΜΜΑ PGP (PRETTY GOOD PRIVACY) ... 469
Α.1. ΕΙΣΑΓΩΓΗ ... 470
Α.2. ΒΑΣΙΚΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ... 471
Α.3. ΕΓΚΑΤΑΣΤΑΣΗ ... 472
Α.3.1. Αρχική Εγκατάσταση σε περιβάλλον Microsoft Windows 2000 ... 472
Α.3.2. Δημιουργία PGP κρυπτογραφικών κλειδιών ... 476
Α.3.3. Ταυτοποίηση των PGP κρυπτογραφικών κλειδιών ... 479
Α.3.4. Κρυπτογράφηση αρχείων με το PGP ... 480
Α.3.4.1. Ρυθμίσεις του PGP ... 480
Α.3.4.2. Εισαγωγή δημόσιου PGP κλειδιού ... 481

Β. ΠΑΡΑΡΤΗΜΑ -ΡΥΘΜΙΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ MICROSOFT WINDOWS 2000 ... 483
Β.1. ΕΙΣΑΓΩΓΗ ... 484
Β.2. ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ ΛΕΙΤΟΥΡΓΙΚΟΥ ΣΥΣΤΗΜΑΤΟΣ MICROSOFT WINDOWS 2000 ... 484
Β.2.1. Εγκατάσταση του τελευταίου Service Pack ... 485
Β.2.2. Εγκατάσταση όλων των απαραίτητων εφαρμογών ... 485
Β.2.3. Επανεγκατάσταση του τελευταίου Service Pack ... 485
Β.2.4. Εγκατάσταση των απαραίτητων Security Bulletin Fixes που δεν καλύπτονται από το τρέχον Service Pack ... 486
Β.3. ΡΥΘΜΙΣΕΙΣ ΤΩΝ ΔΙΚΤΥΑΚΩΝ ΥΠΗΡΕΣΙΩΝ ΚΑΙ ΠΡΩΤΟΚΟΛΛΩΝ ... 486
Β.3.1. Απενεργοποίηση των μη-χρήσιμων δικτυακών υπηρεσιών ... 486
Β.3.2. Απενεργοποίηση του πρωτοκόλλου NetBios ... 487
Β.3.3. Απενεργοποίηση μη-χρησιμοποιούμενων υπηρεσιών και διαδικασιών ... 487
Β.4. ΡΥΘΜΙΣΕΙΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΑΡΧΕΙΩΝ ... 487
Β.4.1. Απενεργοποίηση των προκαθορισμένων ρυθμίσεων του συστήματος αρχείων ... 487
Β.4.2. Ρύθμιση πρόσβασης στη βάση SAM ... 489
Β.4.3. Εφαρμογή Λιστών Ελέγχου Προσπέλασης ... 489

Β.4.4. Διαγραφή των επικίνδυνων εκτελέσιμων αρχείων 490
Β.5. ΡΥΘΜΙΣΕΙΣ ΤΗΣ REGISTRY 491
Β.5.1. Ρυθμίσεις ασφάλειας της Registry 491
Β.5.2. Δικαιώματα προσπέλασης της Registry 496
Β.6. ΕΦΑΡΜΟΓΗ ΠΟΛΙΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ 498
Β.6.1. Account Policies 498
Β.6.2. Local Policies 499
Β.7. ΠΑΡΑΤΗΡΗΣΕΙΣ 500
Βιβλιογραφία 503
Γλωσσάριο 513
Ευρετήριο 519