ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ..... 7

ΚΕΦΑΛΑΙΟ 1: Στοιχεία Κρυπτογραφίας 11

1.1 Εισαγωγή.....11
1.2 Συμμετρική Κρυπτογραφία 12
1.2.1 Παραδείγματα Αλγορίθμων Συμμετρικής Κρυπτογραφίας 13
1.3 Κρυπτογραφία Δημοσίου Κλειδιού.....15
1.3.1 Παραδείγματα Αλγορίθμων Ασύμμετρης Κρυπτογραφίας.....17
1.4 Βασικοί Μηχανισμοί και Διαδικασίες Κρυπτογραφίας 18
1.4.1 Συμφωνία κλειδιών 18
1.4.2 Συναρτήσεις κατακερματισμού.....21
1.4.3 Αλγόριθμοι κρυπτογράφησης τμημάτων 24
1.4.4 Αλγόριθμοι κρυπτογράφησης ροών.....26
1.4.5 Ψηφιακές υπογραφές.....28
1.4.6 Κώδικες Αυθεντικοποίησης Μηνυμάτων 30

ΚΕΦΑΛΑΙΟ 2: Λύσεις και Τεχνολογίες Ασφάλειας 33

2.1 Εισαγωγή.....33
2.2 Υποδομές Δημοσίου Κλειδιού (ΥΔΚ) 33
2.2.1 Βασικές αρχές και ορισμοί.....34
2.2.2 Χρόνος και θέσεις λειτουργίας Έμπιστων Τρίτων Οντοτήτων.....35
2.2.3 Υπηρεσίες και πρότυπα.....37
2.2.4 Οργανωτικά θέματα 42
2.2.5 Νομικό πλαίσιο 45
2.2.6 Η εξέλιξη των Υποδομών Δημοσίου Κλειδιού 47
2.3 Πρωτόκολλα Ασφάλειας Καναλιών.....55
2.3.1 Το πρωτόκολλο Secure Sockets Layer - SSL.....55
2.3.2 Το πρωτόκολλο Transport Layer Security – TLS 60
2.4 Μηχανισμοί Ασφάλειας Ισχυρής Αυθεντικοποίησης.....63
2.4.1 Βιομετρικά συστήματα.....63
2.4.2 Έξυπνες Κάρτες 70

2.5 Ασφάλεια Εφαρμογών....75
2.5.1 Το πλαίσιο ασφάλειας Microsoft Authenticode....75
2.5.2 Ασφάλεια Java....80
2.5.3 Ασφάλεια XML....83
2.6 Ασφάλεια στις Υπηρεσίες Ιστού....111
2.6.1 Εισαγωγή στις Υπηρεσίες Ιστού....111
2.6.2 Ασφάλεια Υπηρεσιών Ιστού (WS-Security)....123
2.6.3 Διαχείριση κλειδιού με XML....126
2.6.4 Γλώσσα Προδιαγραφής Ισχυρισμών Ασφάλειας....130
2.6.5 Επεκτάσιμη Γλώσσα Ελέγχου Πρόσβασης....133
2.6.6 Προηγμένα πρότυπα ασφάλειας Υπηρεσιών Ιστού....136

ΚΕΦΑΛΑΙΟ 3: Εφαρμογή των Τεχνολογιών Ασφάλειας στα Σύγχρονα Π.Σ. 137

3.1 Εισαγωγή....137
3.2 Ασφάλεια στο Διαδίκτυο....137
3.3 Ασφάλεια σε Αρχιτεκτονικές Υπηρεσιών....141
3.3.1 Απαιτήσεις ασφάλειας ΑΠΥ....141
3.3.2 Υπηρεσίες ασφάλειας σε μια ΑΠΥ....142
3.4 Ασφάλεια στα Ασύρματα Π.Σ.....143
3.4.1 Νέες απειλές και προκλήσεις των ασύρματων Π.Σ.....143
3.4.2 Μέθοδοι διασφάλισης εφαρμογών και επικοινωνιών σε ασύρματα Π.Σ....145
3.4.3 Πολιτικές ασφάλειας σε ασύρματα Π.Σ....147
3.4.4 Το μέλλον των ασύρματων Π.Σ.: Ασύρματες Υπηρεσίες Ιστού και Ασύρματες Αρχιτεκτονικές Προσανατολισμένες στις Υπηρεσίες....148

ΚΕΦΑΛΑΙΟ 4: Ασφάλεια Εφαρμογών – Βέλτιστες Πρακτικές και Παραδείγματα.... 149

4.1 Εισαγωγή....149
4.2 Μια ΥΔΚ για τον Τομέα της Ιατρικής Φροντίδας....149
4.3 Υπηρεσία Έκδοσης Ηλεκτρονικών Τιμολογίων - Selis....151
4.3.1 Εισαγωγή....151
4.3.2 Τρέχουσα κατάσταση και νομικό πλαίσιο υπηρεσιών η-τιμολόγησης....152

4.3.3 Η ασφαλής επιχειρησιακή υπηρεσία η-τιμολόγησης SELIS 155
4.4 Υπηρεσία Έκδοσης Εγγράφων Πιστοποίησης Μητρώου Διαμονής για Δήμους - Emayor.....158
4.4.1 Εισαγωγή.....158
4.4.2 Η πλατφόρμα η-διακυβέρνησης eMayor.....159

ΚΕΦΑΛΑΙΟ 5: Εργαστηριακές Ασκήσεις 163

5.1 Εισαγωγή.....163
5.2 Αλγόριθμοι Κρυπτογραφίας - Cryptool 163
5.2.1 CrypTool 163
5.2.2 Εργαστηριακές ασκήσεις 164
5.3 Διαχείριση Πιστοποιητικών – Openssl.....166
5.3.1 Η βιβλιοθήκη και τα εργαλεία OpenSSL 166
5.3.2 Μορφές αρχείων εισόδου και εξόδου.....171
5.3.3 Πρότυπα ελέγχου ανακληθέντων πιστοποιητικών 171
5.3.4 Τα πρότυπα PKCS από RSA Labs 172
5.3.5 Παραδείγματα εργαστηρίου 173
5.3.6 Εργαστηριακές ασκήσεις 178
5.4 Βοηθητικές Υπηρεσίες – Υπηρεσία Καταλόγου.....181
5.4.1 Εισαγωγή στις υπηρεσίες καταλόγου.....181
5.4.2 Lightweight Directory Access Protocol (LDAP) 181
5.4.3 Η λειτουργία του LDAP.....183
5.4.4 LDAP Browser.....184
5.4.5 Χρήση Εντολών openldap.....184
5.4.6 Τα αρχεία διαμόρφωσης Openldap 186
5.4.7 Εργαστηριακές ασκήσεις 187
5.5 Διαχείριση Κλειδιών στη Java - Keytool 188
5.5.1 Περιγραφή keytool.....188
5.5.2 Γενική Χρήση Keytool.....189
5.5.3 Παραδείγματα Εργαστηρίου 191
5.5.4 Εργαστηριακές ασκήσεις 192
5.6 Ασφάλεια Xml.....194
5.6.1 Εργαλεία.....194
5.6.2 Παραδείγματα Εργαστηρίου 194

5.6.3 Εργαστηριακές ασκήσεις 196
5.7 Δικτυακή Ασφάλεια 196
5.7.1 Εισαγωγή....196
5.7.2 Ενότητα 1: Tcpdump....197
5.7.3 Ενότητα 2: NETFILTER / IPTABLES 206
5.7.4 Ενότητα 3 - Snort 216

ΑΝΑΦΟΡΕΣ 221