

# ΠΕΡΙΕΧΟΜΕΝΑ

## Ενότητα 1

### ΒΑΣΙΚΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

<b>1. Βασικές Έννοιες</b>	15
1.1. Εισαγωγή	15
1.2. Τι είναι η Ασφάλεια των Πληροφοριακών Συστημάτων;	16
1.3. Θεμελιώδεις Έννοιες	18
1.3.1. Εμπιστευτικότητα	18
1.3.2. Ακεραιότητα	18
1.3.3. Διαθεσιμότητα	19
1.4. Δευτερεύουσες έννοιες	19
1.4. Παραβάσεις Ασφάλειας	20
1.5. Ευπάθειες	21
1.5.1. Φυσικές Ευπάθειες	21
1.5.2. Εκ Φύσεως Ευπάθειες	22
1.5.3. Ευπάθειες Υλικού και Λογισμικού	22
1.5.4. Ευπάθειες Μέσων	22
1.5.5. Ευπάθειες Εκπομπών	22
1.5.6. Ευπάθειες Επικοινωνιών	22
1.5.7. Ανθρώπινες Ευπάθειες	23
1.6. Απειλές	23
1.6.1. Είδη απειλών	23
1.6.2. Κατηγορίες απειλών	25
1.7. Μέτρα Προστασίας	27
1.7.1. Κατηγορίες Μέτρων Προστασίας	26
1.7.2. Τύποι Μέτρων Προστασίας	27
1.7.3. Αποτελεσματικότητα των μέτρων προστασίας	28
1.7.4. Τοποθέτηση των Μέτρων Προστασίας	29
1.8. Απαιτήσεις Ασφάλειας ΠΣ	30

1.9. Ασφάλεια των Πληροφοριών που Διακινούνται στο Διαδίκτυο	30
1.10. Προβλήματα κατά την Εισαγωγή Ασφάλειας	31
1.11. Αναγκαιότητα και Σκοπιμότητα της Ασφάλειας	31
1.12. Προστασία των Προσωπικών Δεδομένων - Νόμος 2472/97	32
<b>2. Πολιτικές και Μοντέλα Ασφάλειας ΠΣ</b>	
2.1. Ασφαλές ή Έμπιστο Σύστημα;	33
2.2. Πολιτικές και Μηχανισμοί Ασφάλειας	33
2.3. Μοντέλα Ασφάλειας	34
2.3.1. Το Δικτυωτό Μοντέλο	35
2.3.2. Το Μοντέλο Εμπιστευτικότητας Bell-La Padula	36
2.3.3. Το Μοντέλο Ακεραιότητας Biba	39
2.3.4. Το Μοντέλο Graham-Denning	40
2.3.5. Το Μοντέλο Harrison-Ruzzo-Ullman	41
2.3.6. Μοντέλα Ροής-Πληροφοριών	43
2.3.7. Μοντέλα Αποτροπής-Παρεμβολών	43
2.4. Πολιτικές Ασφάλειας Υψηλού Επιπέδου	44
<b>3. Αναγνώριση και Αυθεντικοποίηση</b>	
3.1. Αναγνώριση και Αυθεντικοποίηση Χρήστη	47
3.1.1. Αναγνώριση	47
3.1.2. Αυθεντικοποίηση	47
3.2. Τεχνικές Αυθεντικοποίησης	48
3.2.1. Αυθεντικοποίηση από κάτι που έχει ο χρήστης	48
3.2.2. Αυθεντικοποίηση από χαρακτηριστικά του χρήστη	55
<b>4. Έλεγχος Προσπέλασης</b>	
4.1. Συστήματα Ελέγχου Προσπέλασης	61
4.1.1. Υποκείμενα και αντικείμενα	62
4.1.2. Τύποι Ελέγχου	62
4.1.3. Είδη Προσπέλασης	63
4.1.4. Δικαιώματα Προσπέλασης και Ιδιότητες	63
4.2. Παραδείγματα Συστημάτων Ελέγχου Προσπέλασης	64
4.2.1. Έλεγχος Προσπέλασης στο Λ.Σ. Unix	64
4.2.2. Έλεγχος Προσπέλασης στο Λ.Σ. Windows NT	65
4.3. Διαχείριση Ελέγχου Προσπέλασης	65
4.4. Δομές Ελέγχου Προσπέλασης	65

4.4.1. Πίνακας Ελέγχου Προσπέλασης	66
4.4.2. Ικανότητες	66
4.4.3. Λίστες Ελέγχου Προσπέλασης	67
4.5. Κατηγορίες Πολιτικών Ελέγχου Προσπέλασης	67
4.5.1. Κατά-Απαίτηση Πολιτικές	68
4.5.2. Κατά-Διάκριση Πολιτικές	70
4.5.3. Πολιτικές Βασισμένες-σε-Ρόλους	73
<b>5. Κακόβουλα Προγράμματα</b>	
5.1. Εισαγωγή	77
5.2. Ιοί	78
5.2.1. Ιοί Εκκίνησης	79
5.2.2. Παρασιτικοί Ιοί	80
5.2.3. Συμπληρωματικοί Ιοί	81
5.2.4. Ιοί Μακροεντολών	81
5.2.5. Παράδειγμα από την Ειδησεογραφία	82
5.2.6. Υπογραφές των Ιών	83
5.2.7. Στρατηγική Αντιμετώπισης των Ιών	84
5.3. Σκουλήκια	85
5.4. Δούρειοι Ίπποι	86

## Ε ν ό τ η τ α 2

### ΕΙΔΙΚΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

<b>6. Προστασία Πληροφοριακών Συστημάτων</b>	
6.1. Η έννοια και δομή ενός Πληροφοριακού Συστήματος	91
6.2. Αναγκαιότητα Προστασίας των Πληροφοριακών Συστημάτων	93
6.3. Μοντέλα Ασφάλειας Πληροφοριακών Συστημάτων	94
6.3.1. Μοντέλο του Κιβωτισμού	94
6.3.2. Μοντέλο του Καταλόγου	95
6.3.3. Μοντέλο του Πίνακα	95
6.3.4. Μοντέλο του Φίλτρου	96
6.3.5. Μοντέλο των Επάλληλων Στρωμάτων	96
6.3.6. Αξιολόγηση των μοντέλων	97

<b>7. Ανάλυση Κινδύνων</b>	
7.1. Αναγκαιότητα - Σκοπιμότητα	99
7.2. Βασικές έννοιες	100
7.2.1. Πιθανότητα Πραγματοποίησης Απώλειας	100
7.2.2. Επιπτώσεις από Πιθανή Απώλεια	100
7.2.3. Επιβάρυνση για Πρόληψη Απώλειας	100
7.3. Ο Τύπος BPL	101
7.4. Παράδειγμα Εφαρμογής του Τύπου BPL	102
7.5. Ανάλυση Κινδύνων ΠΣ	102
7.5.1. Σχετικοί Όροι	103
7.5.2. Εφαρμογή BPL σε ΠΣ	105
7.5.3. Παράδειγμα Ανάλυσης Κινδύνων σε ΠΣ	106
<b>8. Ασφάλεια Συστημάτων Βάσεων Δεδομένων</b>	
8.1. Συστήματα Βάσεων Δεδομένων	109
8.2. Παράμετροι Ασφάλειας	110
8.3. Γενικές Αρχές	111
8.4. Απαιτήσεις Ασφάλειας ΣΒΔ	113
8.5. Ασφάλεια Σχεσιακών Βάσεων Δεδομένων	114
8.5.1. Σχεσιακές Βάσεις Δεδομένων	114
8.5.2. Η Γλώσσα SQL	114
8.5.3. Το Μοντέλο Ασφάλειας της SQL	115
8.6. Πολιτικές Ασφάλειας Βάσεων Δεδομένων	117
8.6.1. Η Πολιτική Ασφάλειας Πολλαπλών Επιπέδων	117
8.6.2. Η Κατά-Διάκριση Πολιτική Ασφάλειας	119
8.6.3. Η Πολιτική Ασφάλειας Προσωπικής Γνώσης	120
8.7. Σχέσεις Ασφάλειας μεταξύ ΣΒΔ και ΛΣ	120
8.8. Αξιολόγηση Επιπέδου Ασφάλειας ΣΒΔ	121
8.9. Μέθοδοι Ανάπτυξης Ασφαλών ΣΒΔ	121
8.9.1. Αξιοποίηση Μηχανισμών Ασφάλειας ΣΔΒΔ	121
8.9.2. Βελτίωση των Υφιστάμενων Μηχανισμών Ασφάλειας του ΣΔΒΔ	122
8.9.3. Χρήση Ασφαλών ΣΔΒΔ	123
8.10. Σχεδιασμός Συστημάτων Ασφαλών Βάσεων Δεδομένων	123
8.10.1. Προκαταρκτική Ανάλυση	125
8.10.2. Ανάλυση των Απαιτήσεων Ασφάλειας	126
8.10.3. Σχεδιασμός του Λογικού Μοντέλου της Βάσης Δεδομένων	127

8.10.4. Λογικός Σχεδιασμός της Βάσης Δεδομένων	128
8.10.5. Φυσικός Σχεδιασμός της Βάσης Δεδομένων	128
8.11. Μηχανισμοί Ασφάλειας σε Γνωστά ΣΔΒΔ	129
8.11.1. Περιορισμοί Ακεραιότητας	129
8.11.2. Αυθεντικοποίηση και Έλεγχος Προσπέλασης	133
8.11.3. Προνόμια Προσπέλασης	135
8.11.4. Διαχείριση Προνομίων με Ρόλους	146
<b>9. Ασφάλεια Συστημάτων Κινητής Υπολογιστικής</b>	
9.1. Λειτουργικά Χαρακτηριστικά Κινητής Υπολογιστικής	153
9.1.1. Επικοινωνιακή Υποδομή	154
9.1.2. Λειτουργικά Προβλήματα	157
9.2. Προβλήματα Ασφάλειας ΣΚΥ	158
9.2.1. Ασφάλεια Κατανεμημένων Υπολογιστικών Συστημάτων	158
9.2.2. Κίνδυνοι Ασφάλειας ΣΚΥ	161
9.2.3. Ταξινόμηση Κινδύνων και Ευπαθειών ΣΚΥ	163
9.3. Χειρισμοί Ασφάλειας για ΣΚΥ	165
9.3.1. Ασφάλεια Κινητών Μονάδων	165
9.3.2. Ασφάλεια Κινητών Επικοινωνιών	166
9.3.3. Ασφάλεια Ενσύρματων Δικτύων Υποδομής	167
<b>10. Αξιολόγηση της Ασφάλειας Υπολογιστικών Συστημάτων</b>	
10.1. Πρότυπα και Κριτήρια Αξιολόγησης Ασφάλειας Υπολογιστικών Συστημάτων	170
10.2. Τα Κριτήρια Αξιολόγησης TCSEC	170
10.3. Τα Κριτήρια Αξιολόγησης ITSEC	173
<b>Ε ν ό τ η τ α 3</b>	
<b>ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΤΩΝ ΣΥΝΑΛΛΑΓΩΝ ΣΕ ΔΙΚΤΥΑΚΟ ΠΕΡΙΒΑΛΛΟΝ</b>	
<b>11. Ασφάλεια των Πληροφοριών στο Διαδίκτυο</b>	
11.1. Δίκτυα και Διαδίκτυο	177
11.2. Προβλήματα Ασφάλειας Δικτύων	178
11.3. Ασφάλεια και Διαδίκτυο	179
11.3.1. Κίνδυνοι Ασφάλειας	179
11.3.2. Εγγενή Προβλήματα Ασφάλειας	180

11.3.3. Απειλές Ασφάλειας	180
11.3.4. Είδη Επιθέσεων	181
11.4. Βασικοί Χειρισμοί Ασφάλειας	182
<b>12. Κρυπτογραφία</b>	
12.1. Ορισμοί	187
12.2. Τυπικό Σύστημα Κρυπτογράφησης	188
12.2.1. Ιδιότητες των Κλειδιών	189
12.2.2. Ανάλυση Ανθεκτικότητας των Αλγορίθμων	190
12.2.3. Χρήσεις των Κρυπτογραφικών Συστημάτων	191
12.3. Κρυπτογραφικοί Αλγόριθμοι	191
12.3.1. Τύποι Κρυπτογραφικών Αλγορίθμων	192
12.3.2. Κρυπτογραφικοί Αλγόριθμοι Ροής	192
12.3.3. Κρυπτογραφικοί Αλγόριθμοι Δέσμης	200
<b>13. Προστασία Ψηφιακών Επικοινωνιών</b>	
13.1. Βασικά Θέματα Προστασίας	203
13.2. Κρυπτογραφία Μυστικού Κλειδιού	204
13.2.1. Κρυπτογραφικός Αλγόριθμος DES	205
13.2.2. Κρυπτογραφικός Αλγόριθμος Triple-DES	207
13.2.3. Κρυπτογραφικός Αλγόριθμος IDEA	207
13.2.4. Κρυπτογραφικοί Αλγόριθμοι RC2 και RC4	208
13.2.5. Κρυπτογραφικός Αλγόριθμος AES	208
13.3. Κρυπτογραφία Δημόσιου Κλειδιού	208
13.3.1. Συμμετρική ή Ασύμμετρη Κρυπτογράφηση;	209
13.3.2. Τρόποι Κρυπτογράφησης Δημοσίου Κλειδιού	210
13.3.3. Κρυπτογραφικό Σύστημα RSA	212
13.3.4. Εφαρμογές της Κρυπτογράφησης Δημοσίου Κλειδιού	214
13.3.5. Συνολική Διαδικασία Κρυπτογράφησης	215
<b>14. Υποδομές Πιστοποίησης</b>	
14.1. Εισαγωγή στα Ψηφιακά Πιστοποιητικά	219
14.2. Τύποι Ψηφιακών Πιστοποιητικών	220
14.3. Αρχές και Ιεραρχίες Πιστοποίησης	220
14.3.1. Αρχές Πιστοποίησης	220
14.3.2. Ιεραρχίες Πιστοποίησης	220
14.4. Υποδομή Δημοσίου Κλειδιού	224

14.4.1. Σκοπός - Αναγκαιότητα	224
14.4.2. Συστατικά μέρη της Υποδομής Δημόσιου Κλειδιού	225
14.4.3. Υπηρεσίες Υποδομής Δημόσιου Κλειδιού	227
<b>15. Ασφαλείς Συναλλαγές στο Διαδίκτυο</b>	
15.1. Εισαγωγή	229
15.2. Απαιτήσεις Ασφάλειας	230
15.3. Ασφαλές Σύστημα Συναλλαγών	230
15.4. Το Σύστημα Ηλεκτρονικών Συναλλαγών SET	231
15.5. Σχεδιασμός Ολοκληρωμένων Συστημάτων Συναλλαγών	233
15.6. Υλοποίηση Ολοκληρωμένου Συστήματος Συναλλαγών	236
<b>16. Ασφάλεια Εφαρμογών Διαδικτύου</b>	
16.1. Το πρωτόκολλο SSL	240
16.2. Τρόπος Λειτουργίας του SSL	241
16.3. Επιβάρυνση από τη Χρήση του SSL	243
16.4. Ενεργοποίηση SSL	244
<b>17. Προστασία με Firewalls</b>	
17.1. Σκοπιμότητα	245
17.2. Ορισμοί	246
17.3. Παρεχόμενη Ασφάλεια	247
17.4. Βασικές Τεχνικές Προστασίας	248
17.5. Σύγχρονες τεχνολογίες Firewalls – Υβριδικές πύλες	253
17.6. Σύγκριση Τεχνικών Προστασίας	254
17.7. Αρχιτεκτονικές Συστημάτων Firewalls	255
17.8. Γενικές Κατευθύνσεις Πολιτικής Ασφάλειας	256
17.9. Πλεονεκτήματα και Περιορισμοί	258
17.9.1. Πλεονεκτήματα από τη Χρήση Firewalls	258
17.9.2. Περιορισμοί των Firewalls	260
17.10. Αποδεκτή Λειτουργικότητα Συστημάτων Firewalls	261

#### Ενότητα 4

### ΤΕΧΝΙΚΕΣ ΚΑΙ ΠΑΡΑΔΕΙΓΜΑΤΑ ΕΦΑΡΜΟΓΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

#### 18. Παράδειγμα - Εφαρμογή Μεθόδων και Τεχνικών Προστασίας ΠΣ

18.1. Κατηγορίες Μεθόδων και Τεχνικών Προστασίας	265
18.2. Σε περίπτωση Έκτακτης Ανάγκης	265
18.2.1. Περιπτώσεις Δυσλειτουργίας	265
18.2.2. Περιπτώσεις Ολικής Καταστροφής	266
18.3. Κατά τις Καθημερινές Διεργασίες	266
18.3.1. Φυσική Προστασία	267
18.3.2. Λογική Προστασία	268
18.3.3. Προστασία Βασικών Δικτύων και Εξοπλισμού Συναλλαγών	271
18.3.4. Προστασία Λοιπών Δικτύων, Περιφερειακού και Βοηθητικού Εξοπλισμού	273
<b>19. Παραδείγματα Εισαγωγής Ασφάλειας σε Συστήματα ΒΔ</b>	
19.1. Παράδειγμα Ασφαλούς Σχεδιασμού Βάσεων Δεδομένων	275
19.2. Παράδειγμα Εισαγωγής Περιορισμών Ακεραιότητας	278
19.2.1. Χρησιμότητα	278
19.2.2. Εφαρμογή των Περιορισμών Ακεραιότητας	280
19.3. Παραδείγματα Διαχείρισης Προνομίων και Ρόλων	282
19.3.1. Προστασία Πινάκων	283
19.3.2. Προστασία με Χρήση Απόψεων	286
19.3.3. Περιορισμοί στην Παραχώρηση Προνομίων με Ρόλους	287
<b>20. Παράδειγμα Διαχείρισης Ψηφιακών Πιστοποιητικών και Υπογραφών</b>	
20.1. Προϋποθέσεις για την Απόκτηση Ψηφιακού Πιστοποιητικού / Υπογραφής	297
20.2. Απόκτηση Ψηφιακού Πιστοποιητικού / Υπογραφής	298
20.2.1. Πρότυπα Αρχείων Πιστοποιητικών	298
20.3. Υπογραφή και Κρυπτογράφηση Μηνυμάτων	299
20.4. Εισαγωγή και Εξαγωγή Ψηφιακής Υπογραφής	299
20.4.1. Εισαγωγή στο Netscape Communicator	300
20.4.2. Εισαγωγή στο Microsoft Internet Explorer	302
20.4.3. Εξαγωγή από το Netscape Communicator	307
20.4.4. Εξαγωγή από το Microsoft Internet Explorer	309
20.5. Υπογραφή και Κρυπτογράφηση Μηνυμάτων	314
20.5.1. Με το Netscape Messenger	315
20.5.2. Με το Outlook Express	318



---

<b>21. Παράδειγμα Ανάπτυξης Ασφαλούς Εφαρμογής στο Διαδίκτυο</b>	
21.1. Δομικά Στοιχεία	322
21.2. Λειτουργική Περιγραφή	322
21.3. Αυθεντικοποίηση Εξυπηρετητή	322
21.3.1. Απόκτηση ηλεκτρονικού πιστοποιητικού	323
21.4. Αυθεντικοποίηση Πελάτη	328
21.5. Έλεγχος πρόσβασης	328
21.5.1. Εξυπηρετητές Καταλόγου	329
21.5.2. Certificate Realms	330
21.5.3. Προστασία Εικονικών Μονοπατιών	330
21.6. Συμπεράσματα	332
<b>Βιβλιογραφία</b>	<b>335</b>