Πίνακας Περιεχομένων

Κεφάλαιο 0 - Εισαγωγικό Σημείωμα 25

0.1. Εισαγωγή 25

0.2. Συγγραφείς κεφαλαίων του συλλογικού τόμου 26

Κεφάλαιο 1 – Εισαγωγή στην Ασφάλεια Πληροφοριών και Συστημάτων στον Κυβερνοχώρο 31

1.1. Εισαγωγή 31

1.2. Όροι και ορισμοί 34

1.3. Οργάνωση της ύλης του βιβλίου 42

Πρώτο Μέρος 43

Δεύτερο Μέρος 44

Τρίτο Μέρος 44

Τέταρτο Μέρος 45

1.4. Σύνοψη 46

Βιβλιογραφικές Αναφορές 46

ΜΕΡΟΣ Α - Οργανωσιακές, Κανονιστικές και Ανθρώπινες Πτυχές της Ασφάλειας Πληροφοριών 47

Κεφάλαιο 2 – Διακυβέρνηση και Διοίκηση Ασφάλειας Πληροφοριών 49

2.1. Εισαγωγή 50

2.2. Διακυβέρνηση ασφάλειας πληροφοριών 52

2.3. Διοίκηση ασφάλειας πληροφοριών 54

2.3.1. Γενικά....54
2.3.2. Πολιτικές ασφάλειας πληροφοριών....56
2.3.3. Οργάνωση της ασφάλειας πληροφοριών....58
2.3.4. Ανθρώπινο δυναμικό....59
2.3.5. Διαχείριση περιουσιακών στοιχείων....60
2.3.6. Έλεγχος πρόσβασης....60
2.3.7. Κρυπτογραφία....61
2.3.8. Φυσική και περιβαλλοντική ασφάλεια....61
2.3.9. Λειτουργική ασφάλεια....62
2.3.10. Ασφάλεια επικοινωνιών....63
2.3.11. Προμήθεια, ανάπτυξη και συντήρηση συστημάτων....64
2.3.12. Σχέσεις με προμηθευτές....64
2.3.13. Διαχείριση επεισοδίων ασφάλειας πληροφοριών....64
2.3.14. Ασφάλεια πληροφοριών και επιχειρησιακή συνέχεια....65
2.3.15. Συμμόρφωση....66
2.3.16. Άλλες διαστάσεις της διοίκησης ασφάλειας πληροφοριών....67

2.4. Διαχείριση επικινδυνότητας....68

2.4.1. Επικινδυνότητα και συναφείς έννοιες....68
2.4.2. Η μεθοδολογία της διαχείρισης επικινδυνότητας πληροφοριακών συστημάτων....70
2.4.3. Πλεονεκτήματα και μειονεκτήματα....72

2.5. Σύνοψη....73

Βιβλιογραφικές Αναφορές....74

Κεφάλαιο 3 – Το Κανονιστικό Πλαίσιο της (Κυβερνο)Ασφάλειας....75

3.1. Η (Κυβερνο)Ασφάλεια ως αντικείμενο ρύθμισης....76

3.2. Κανονιστικός ορισμός της (κυβερνο)ασφάλειας....77

3.3. Η ρύθμιση της ασφάλειας στην Οδηγία για την Κυβερνοασφάλεια (Οδηγία NIS) και στην εθνική νομοθεσία....78

3.3.1. Εθνική στρατηγική για την ασφάλεια....80
3.3.2. Μηχανισμοί εφαρμογής και συνεργασίας....81

3.3.3. Σύγκλιση των στρατηγικών και επιπέδων ασφάλειας;....82
3.3.4. Οι κανονιστικές απαιτήσεις ως προς την ασφάλεια συστημάτων, δικτύων και πληροφοριών....83
3.3.5. Η υποχρέωση κοινοποίησης συμβάντων ασφάλειας....85
3.3.6. Οι κυρώσεις....87
3.4. Η Πράξη για την Κυβερνοασφάλεια (Cybersecurity Act)....88
3.4.1. Ο ρόλος του ENISA....89
3.4.2. Το πλαίσιο για την πιστοποίηση κυβερνοασφάλειας....90
3.5. Οι απαιτήσεις ασφάλειας στον Γενικό Κανονισμό Προστασίας Δεδομένων....93
3.5.1. Η σχέση της ασφάλειας και της προστασίας προσωπικών δεδομένων....93
3.5.2. Η αρχή και οι απαιτήσεις ασφάλειας στον Γενικό Κανονισμό Προστασίας Δεδομένων....94
3.5.3. Η υποχρέωση γνωστοποίησης/ανακοίνωσης παραβιάσεων (ασφάλειας) δεδομένων....97
3.6. Σύνοψη....99
Βιβλιογραφικές Αναφορές....101

Κεφάλαιο 4 – Ασφάλεια Πληροφοριακών Συστημάτων και Ανθρώπινος Παράγοντας....105

4.1. Εισαγωγή....106
4.2. Η κοινωνικοτεχνική προσέγγιση στην Ασφάλεια Πληροφοριακών Συστημάτων....109
4.3. Ο πολυδιάστατος ρόλος του ανθρώπινου παράγοντα....111
4.3.1. Ο άνθρωπος ως αδυναμία: ο ασθενέστερος κρίκος της ασφάλειας....111
4.3.2. Ο άνθρωπος ως απειλή ασφάλειας....112
4.3.3. Ο άνθρωπος ως μέτρο προστασίας: Ο ρόλος των προγραμμάτων ενημερότητας ασφάλειας....114
4.4. Συμπεριφορά ασφάλειας χρηστών....117
4.5. Εύχρηστη ασφάλεια (usable security)....120

4.5.1. Η έννοια και η σημασία της ευχρηστίας....120
4.6. Σύνοψη και συμπεράσματα....123
Βιβλιογραφικές Αναφορές....124

Κεφάλαιο 5 – Μοντέλα Επιθέσεων και Επιτιθέμενων 129
5.1. Εισαγωγή....129
5.2. Δένδρα επιθέσεων....131
5.3. Μοντέλο επιθέσεων STRIDE....132
5.4. Μοντέλο Επιθέσεων NIST....134
5.5. Μοντέλο Επιτιθέμενων Intel TAL....136
5.5.1. Χαρακτηριστικά Επιτιθέμενου....137
5.5.2. Κατηγορίες Επιτιθέμενων....140
5.6. Μοντέλο Επιθέσεων/Επιτιθέμενων OCTAVE....142
5.7. Μοντέλο Επιθέσεων PASTA....143
5.8. Μοντέλα Επιθέσεων του οργανισμού MITRE....143
5.8.1. Μοντέλο Επιθέσεων/Επιτιθέμενων PRE-ATT&CK....144
5.8.2. Μοντέλο Επιθέσεων TARA....144
5.8.3. Μοντέλο Επιθέσεων CAPEC....145
5.9. Ταξινόμηση κυβερνοαπειλών της ENISA....146
5.10. Σύνοψη – Συγκριτική παρουσίαση....148
Βιβλιογραφικές Αναφορές....151

Κεφάλαιο 6 – Ιδιωτικότητα και Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας....155
6.1. Εισαγωγή....156
6.2. Περιβάλλον Απειλών κατά της Ιδιωτικότητας και οι Απαιτήσεις για την Προστασία της....159
6.3. Η Ιδιωτικότητα υπό την Οπτική του Φορέα....162
6.3.1. Ικανοποίηση των Αρχών Ιδιωτικότητας και Νομικών Υποχρεώσεων.... 163

6.3.2. Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας από την Πλευρά των Φορέων 168

6.4. Η Ιδιωτικότητα υπό την Οπτική του Χρήστη 172

6.4.1. Ο Χρήστης Σύγχρονων Ηλεκτρονικών Υπηρεσιών 172

6.4.2. Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας από την Πλευρά των Χρηστών 176

6.5. Μελέτες Περίπτωσης και Συζήτηση 178

6.5.1. Πληροφοριακό Σύστημα Φοιτητολογίου 178

6.5.2. Πληροφοριακό Σύστημα Διαχείρισης Αποφοίτων 179

6.5.3. Συμμόρφωση του Φορέα με Βασικές Αρχές και Απαιτήσεις 181

6.5.4. Εφαρμογή Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας από τον Φορέα 184

6.5.5. Εφαρμογή Τεχνολογιών Ενίσχυσης της Ιδιωτικότητας από το Χρήστη 185

6.6. Σύνοψη και Συμπεράσματα 188

Βιβλιογραφικές Αναφορές 188

Κεφάλαιο 7 – Η Επίδραση της Εμπειρίας του Χρήστη στην Ασφάλεια και την Προστασία της Ιδιωτικότητας 191

7.1. Εισαγωγή 192

7.2. Βασικές Έννοιες 194

7.2.1. Εμπειρία του χρήστη 194

7.2.2. Ευχρηστία 198

7.2.3. Ασφάλεια Πληροφοριών και Υπολογιστών 200

7.2.4. Εμπειρία του χρήστη και ασφάλεια 203

7.3. Πλαίσια Εύχρηστης Ασφάλειας 204

7.4. Ευχρηστία και Κοινωνικά Δίκτυα 215

7.5. Σύνοψη 223

Βιβλιογραφικές Αναφορές 225

ΜΕΡΟΣ Β - Ασφάλεια Συστημάτων 233

Κεφάλαιο 8 – Εφαρμοσμένη Κρυπτογραφία..... 235

8.1. Εισαγωγή.....236

8.2. Βασικοί όροι.....238

8.2.1. Συμμετρική και ασύμμετρη κρυπτογραφία.....239
8.2.2. Κρυπτογραφικοί στόχοι ασφάλειας.....240
8.2.3. Ασφάλεια κρυπτογραφικών αλγορίθμων και πρωτοκόλλων 242

8.3. Βασικά κρυπτογραφικά δομικά στοιχεία.....244

8.3.1. Κρυπταλγόριθμος τμήματος.....244
8.3.2. Κρυπτογραφικές συναρτήσεις κατακερματισμού 246
8.3.3. Γεννήτριες ψευδοτυχαίων ακολουθιών.....248
8.3.4. Αλγόριθμοι κρυπτογράφησης δημοσίου κλειδιού.....249

8.4. Εφαρμογές συμμετρικής κρυπτογραφίας.....250

8.4.1. Εμπιστευτικότητα δεδομένων 250
8.4.2. Αυθεντικοποίηση δεδομένων 256
8.4.3. Αυθεντικοποιημένη κρυπτογράφηση.....259
8.4.4. Κρυπτογραφία χαμηλών απαιτήσεων σε υπολογιστικούς πόρους.....262

8.5. Εφαρμογές ασύμμετρης κρυπτογραφίας 263

8.5.1. Ψηφιακές υπογραφές.....264
8.5.2. Μηχανισμοί ενθυλάκωσης κλειδιού.....265
8.5.3. Αυθεντικοποίηση οντότητας και πρωτόκολλα μηδενικής γνώσης.....267

8.6. Διαχείριση κλειδιών 269

8.6.1. Μεγέθη κλειδιών 269
8.6.2. Συναρτήσεις παραγωγής κλειδιών.....270
8.6.3. Εγκαθίδρυση κλειδιών 273
8.6.4. Αποθήκευση κλειδιών.....274

8.7. Ειδικά θέματα.....275

8.7.1. Προηγμένη Κρυπτογραφία.....275
8.7.2. Η κρυπτογραφία στην εποχή των κβαντικών υπολογιστών.....278

8.8. Σύνοψη 279

Βιβλιογραφικές Αναφορές 279

Κεφάλαιο 9 – Αυθεντικοποίηση Οντότητας 283

9.1. Εισαγωγικές Παρατηρήσεις 283

9.2. Εννοιολογική Θεμελίωση 285

9.2.1. Αυθεντικότητα: Οντότητες και Απειλές 285

9.2.2. Υπηρεσίες Αυθεντικότητας και Ακεραιότητας 286

9.2.3. Ταυτοποίηση Χρήστη vs Ταυτοποίηση Προγράμματος 287

9.2.4. Συμβολισμοί και Υποθέσεις Ασφάλειας 289

9.3. Αυθεντικότητα Οντότητας με Κωδικούς Προσπέλασης 290

9.3.1. Απειλές κατά Συστημάτων Ταυτοποίησης με Κωδικούς Προσπέλασης και Προτεινόμενα Αντίμετρα 290

9.4. Αυθεντικότητα Οντότητας με Κρυπτογραφικές Τεχνικές 295

9.4.1. Ταυτοποίηση με Πρόκληση-Απάντηση 295

9.4.2. Ταυτοποίηση με Χρονοσφραγίδες 301

9.5. Σύνοψη 303

Βιβλιογραφικές Αναφορές 304

Κεφάλαιο 10 – Έλεγχος Προσπέλασης και Εξουσιοδότηση . 307

10.1. Εισαγωγή 307

10.2. Ορισμοί 309

10.2.1. Επίπεδα Ελέγχου Προσπέλασης 310

10.2.2. Σύστημα Ελέγχου Προσπέλασης 311

10.2.3. Αρχές Εξουσιοδότησης 312

10.3. Κλασικές Προσεγγίσεις Ελέγχου Προσπέλασης 313

10.3.1. MAC: Έλεγχος Προσπέλασης Κατ' Απαίτηση 313

10.3.2. DAC: Έλεγχος Προσπέλασης Κατά Διάκριση 315

10.3.3. RBAC: Έλεγχος Προσπέλασης Βασισμένος σε Ρόλους 318

10.4. Σύγχρονες Προσεγγίσεις Ελέγχου Προσπέλασης 321

10.4.1. ABAC: Έλεγχος Προσπέλασης Βασισμένος σε Χαρακτηριστικά 321
10.4.2. Πρότυπο XACML 324
10.4.3. Πλαίσιο NGAC 326
10.5. Τρέχοντα και ανοιχτά ζητήματα ελέγχου προσπέλασης 330
10.6. Σύνοψη 332
Βιβλιογραφικές Αναφορές 332

Κεφάλαιο 11 – Ασφάλεια στα Λειτουργικά Συστήματα και στην Εικονικοποίηση 337

11.1. Εισαγωγή 338
11.2. Ευπάθειες και Απειλές 339
11.2.1. Αδύναμοι Κωδικοί Προσπέλασης 339
11.2.2. Ευπάθειες Μνήμης 340
11.2.3. Ευπάθειες Συνθηκών Ανταγωνισμού 342
11.3. Μηχανισμοί Ασφάλειας Λειτουργικών Συστημάτων 344
11.3.1. Αυθεντικοποίηση Χρήστη 344
11.3.2. Έλεγχος Προσπέλασης 347
11.3.3. Ακεραιότητα 348
11.4. Αρχές Σχεδίασης Ασφαλών Λειτουργικών Συστημάτων 350
11.4.1. Πεδία ασφάλειας 351
11.4.2. Χαρακτηρισμός ασφάλειας αρχιτεκτονικών ΛΣ 352
11.4.3. Αρχές Saltzer και Schroeder 354
11.5. Ασφάλεια στην εικονικοποίηση 355
11.5.1. Γενικά Χαρακτηριστικά Ασφάλειας στην Εικονικοποίηση 357
11.5.2. Ασφάλεια Επιμέρους Τεχνολογιών Εικονικοποίησης 358
11.6. Σύνοψη 363
Βιβλιογραφικές Αναφορές 363

Κεφάλαιο 12 – Ασφάλεια Βάσεων Δεδομένων 365

12.1. Εισαγωγή 366

12.2. Ευαίσθητα Δεδομένα και Απειλές 367
12.2.1. Ευαίσθητα δεδομένα 367
12.2.2. Απειλές για μια βάση δεδομένων 368
12.3. Μηχανισμοί Ασφάλειας 369
12.4. Έλεγχος Προσπέλασης κατά Διάκριση 371
12.4.1. Δικαιώματα Προσπέλασης στην SQL 372
12.4.2. Δικαιώματα Προσπέλασης για Όψεις 377
12.5. Έλεγχος Προσπέλασης Κατ' Απαίτηση 378
12.6. Άλλα Θέματα Ασφάλειας Βάσεων Δεδομένων 380
12.6.1. Έγχυση SQL 380
12.6.2. Κρυπτογραφία 382
12.7. Σύνοψη 383
Βιβλιογραφικές Αναφορές 384

Κεφάλαιο 13 – Ασφάλεια Κατανεμημένων Συστημάτων .. 385
13.1. Εισαγωγή 386
13.2. Κατηγορίες Κατανεμημένων Συστημάτων 387
13.3. Αποκεντρωμένα Μοντέλα Ομότιμων Κόμβων 388
13.3.1. Κατηγορίες Δικτύων Ομότιμων Κόμβων 389
13.3.2. Μη-δομημένα Πρωτόκολλα Ομότιμων Κόμβων 390
13.3.3. Δομημένα Πρωτόκολλα Ομότιμων Κόμβων 391
13.3.4. Υβριδικά Πρωτόκολλα Ομότιμων Κόμβων 391
13.3.5. Ιεραρχικά Πρωτόκολλα Ομότιμων Κόμβων 391
13.4. Επιθέσεις στα Συστήματα Ομότιμων Κόμβων 392
13.4.1. Τύποι Επιθέσεων 393
13.4.2. Μηχανισμοί ασφάλειας 396
13.5. Συντονισμένη ομαδοποίηση πόρων 397
13.5.1. Έννοιες Κατανεμημένων Συστημάτων και Κατηγορίες Συντονισμού 398
13.5.2. Συντονισμός 398

13.5.3. Συνέπεια 399
13.5.4. Σχήματα Συντονισμού και Διαχείρισης Αντιγράφων 400
13.5.5. Βυζαντινή Ανοχή Σφαλμάτων 401
13.5.6. Πρωτόκολλα Δέσμευσης 402
13.6. Κατηγορίες Συντονισμού και Δυνατότητες Επίθεσης 402
13.6.1. Διαταραχές στα Κατανεμημένα Συστήματα 402
13.6.2. Συντονισμός Πόρων 403
13.6.3. Επιθέσεις και Μηχανισμοί Άμυνας στον Συντονισμό Πόρων 404
13.6.4. Συντονισμός Υπηρεσιών 405
13.6.5. Επιθέσεις και Μηχανισμοί Άμυνας στο Συντονισμό Υπηρεσιών 406
13.7. Σύνοψη 407
Βιβλιογραφικές Αναφορές 407

Κεφάλαιο 14 – Ασφάλεια Δεδομένων Μεγάλου Όγκου .. 411
14.1. Εισαγωγή 412
14.2.1. Η φύση των δεδομένων μεγάλου όγκου 414
14.2.2. Τα χαρακτηριστικά των ΔΜΟ και η επίπτωσή τους στην ασφάλεια 415
14.3. Προκλήσεις στην ασφάλεια των ΔΜΟ 418
14.3.1. Απόκτηση των ΔΜΟ 418
14.3.2. Αποθήκευση των ΔΜΟ 418
14.3.3. Ανάλυση των ΔΜΟ 419
14.4. Απειλές ασφάλειας σε δεδομένα μεγάλου όγκου 420
14.4.1. Απειλές ασφάλειας στις υποδομές των ΔΜΟ 421
14.4.2. Απειλές ασφάλειας κατά τη διαχείριση των ΔΜΟ 422
14.4.3. Απειλές ασφάλειας κατά τη διαχείριση των ΔΜΟ 423
14.5. Μηχανισμοί ασφάλειας και καλές πρακτικές προστασίας Δεδομένων Μεγάλου όγκου 423
14.6. Σύνοψη 425
Βιβλιογραφικές Αναφορές 426

Κεφάλαιο 15 – Ασφάλεια σε Περιβάλλον Αλυσίδας Μπλοκ.. 429

15.1. Εισαγωγή 430

15.1.1. Τεχνολογία Κατανεμημένου Καθολικού 430

15.1.2. Τεχνολογία Αλυσίδας Μπλοκ 431

15.2. Κατηγοριοποίηση των Αλυσίδων Μπλοκ 435

15.2.1. Αλυσίδες Μπλοκ χωρίς Άδεια 436

15.2.2. Αλυσίδες Μπλοκ με Άδεια 437

15.3. Βασικά Χαρακτηριστικά των Αλυσίδων Μπλοκ 439

15.3.1. Συναρτήσεις Σύνοψης/Κατακερματισμού 439

15.3.2. Κρυπτογραφία Δημοσίου Κλειδιού 439

15.3.3. Διευθύνσεις 440

15.3.4. Αλγόριθμος Συναίνεσης 441

15.3.5. Έξυπνα Συμβόλαια 444

15.4. Δημοφιλείς Πλατφόρμες Αλυσίδων Μπλοκ 444

15.4.1. Bitcoin 445

15.4.2. Ethereum 446

15.4.3. Hyperledger Fabric 448

15.5. Ζητήματα Ασφάλειας των Αλυσίδων Μπλοκ 450

15.5.1. Επίθεση Sybil 450

15.5.2. Εγωιστική Εξόρυξη 451

15.5.3. Διακλάδωση Αλυσίδας Μπλοκ 451

15.5.4. Παρωχημένα και Ορφανά Μπλοκ 452

15.5.5. Η Επίθεση του 51% 453

15.5.6. Καθυστέρηση Συναίνεσης 453

15.5.7. Διπλή Δαπάνη 454

15.6. Σύνοψη 454

Βιβλιογραφικές Αναφορές 455

Κεφάλαιο 16 – Ψηφιακή Δικανική 457

16.1. Εισαγωγή 458

16.1.1. Απόδοση ευθυνών στον Κυβερνοχώρο 459

16.1.2. Μελέτη περίπτωσης: APT28 462

16.2. Αρχές Ψηφιακής Δικανικής 463

16.3. Ο Ρόλος των Μεταδεδομένων 466

16.4. Ψηφιακή Δικανική Συστημάτων Αρχείων (File System Forensics) 468

16.4.1. Συλλογή και Ανάλυση 469

16.5. Ψηφιακή Δικανική Εφαρμογών (Application Forensics) 471

16.6. Ψηφιακή Δικανική σε Περιβάλλοντα Νεφοϋπολογιστικής (Cloud Forensics) 473

16.6.1. Διερεύνηση και Αναγνώριση 475
16.6.2. Συλλογή και Ανάλυση 476
16.6.3. Δημιουργία Σεναρίου Περιστατικού 476

16.7. Ψηφιακή Δικανική στο Διαδίκτυο των Πραγμάτων (IoT Forensics) 477

16.8. Ψηφιακή Δικανική σε Δίκτυα Υπολογιστών (Network Forensics) 479

16.8.1. Συλλογή 479
16.8.2. Ανάλυση 481

16.9. Πληροφορίες από Ανοικτές Πηγές (Open Source Intelli-gence) 483

16.10. Σύνοψη 485

Βιβλιογραφικές Αναφορές 485

ΜΕΡΟΣ Γ - Ασφάλεια Λογισμικού 489

Κεφάλαιο 17 – Τεχνολογία Αποτύπωσης Απαιτήσεων Ασφάλειας 491

17.1. Εισαγωγή 492

17.2. Μεθοδολογίες αποτύπωσης απαιτήσεων ασφάλειας 493

17.2.1. Security Quality Requirements Engineering Methodology (SQUARE) 494
17.2.2. Model Oriented Security Requirements Engineering (MOSRE) 494

17.2.3. Security Requirements Engineering Framework (SREF) 495
17.2.4. Eliciting Security Requirements from the Business Process Models 496
17.2.5. Security Requirements Engineering Process (SREP) 496
17.2.6. Secure Tropos 497
17.2.7. KAOS 498
17.2.8. PresSure 499
17.2.9. Goal-based requirements analysis method (GBRAM) 499
17.2.10. Abuse frames 500
17.2.11. Misuse Cases 500
17.2.12. Το πλαίσιο M-N (Moffett - Nuseibeh) 501
17.2.13. Το πλαίσιο NFR (Non-Functional Requirements) 502
17.2.14. Η i* μεθοδολογία 503

17.3. Συγκριτική παρουσίαση τεχνολογιών αποτύπωσης απαιτήσεων ασφάλειας 504

17.4. Νεφοϋπολογιστική και ασφάλεια 508

17.5. Σύνοψη 512

Βιβλιογραφικές Αναφορές 513

Κεφάλαιο 18 – Τεχνολογία Αποτύπωσης Απαιτήσεων Ιδιωτικότητας 517

18.1. Εισαγωγή 518

18.2. Εννοιολογική θεμελίωση 520

18.3. Τεχνολογία αποτύπωσης απαιτήσεων ιδιωτικότητας 522

18.3.1. Η μεθοδολογία LINDDUN 523
18.3.2. Η μεθοδολογία Privacy Safeguard (PriS) 525
18.3.3. Το πλαίσιο Role-Based Access Control (RBAC) 527
18.3.4. Η μέθοδος Security Quality Requirements Engineering (SQUARE) for Privacy 529
18.3.5. Η τεχνική Privacy Requirements Elicitation Technique (PRET) 531
18.3.6. Η μέθοδος Structured Analysis Framework for Privacy (STRAP) 532
18.3.7. Η μεθοδολογία Preparing Industry to Privacy by Design by supporting its Application in Research (PRIPARE) 533

18.3.8. Το πλαίσιο Modeling and Analysis of Privacy-aware Systems (MAPaS) 536
18.3.9. Η μέθοδος Goal-Based Requirements Analysis Method (GBRAM) 537
18.3.10. Η μεθοδολογία Secure Tropos 538
18.4. Σύγκριση τεχνολογιών αποτύπωσης απαιτήσεων ιδιωτικότητας 539
18.5. Σύνοψη 542
Βιβλιογραφικές Αναφορές 543

Κεφάλαιο 19 – Τεχνολογία Ασφαλούς Λογισμικού 547
19.1. Εισαγωγή 547
19.2. Ευπάθειες, επιθέσεις και αντίμετρα 548
19.2.1. Επιθέσεις έγχυσης SQL 549
19.2.2. Επιθέσεις έγχυσης JavaScript 552
19.2.3. Πλαστογράφηση αιτήματος μεταξύ ιστοτόπων 557
19.2.4. Υπερχείλιση προσωρινής μνήμης 561
19.2.5. Εκμετάλλευση συνθηκών ανταγωνισμού 566
19.3. Διαδικασίες και πρακτικές ανάπτυξης ασφαλούς λογισμικού 569
19.4. Σύνοψη 572
Βιβλιογραφικές Αναφορές 573

Κεφάλαιο 20 – Κακόβουλο Λογισμικό 579
20.1. Εισαγωγή 580
20.2. Διασπορά κακόβουλου λογισμικού 586
20.3. Ποικιλομορφία 588
20.4. Αρχεία με κακόβουλο λογισμικό 590
20.5. Διαχείριση ενός botnet 591
20.6. Μέθοδοι ανάλυσης κακόβουλου λογισμικού 593
20.6.1. Στατική ανάλυση 594
20.6.2. Δυναμική ανάλυση 596

20.7. Αντίμετρα 597

20.8. Εντοπισμός κακόβουλου λογισμικού 599

Βιβλιογραφικές Αναφορές 602

Κεφάλαιο 21 – Ασφάλεια στον Παγκόσμιο Ιστό 607

21.1. Εισαγωγή 608

21.2. Κενά ασφάλειας στον Παγκόσμιο Ιστό 609

21.2.1. Εισαγωγή κακόβουλου κώδικα (Code Injection) 610

21.2.2. Εξωτερικές Οντότητες XML (XML External Entities) 611

21.2.3. Ευπαθής ταυτοποίηση χρηστών (Broken Authentication) 612

21.2.4. Ευπαθής έλεγχος πρόσβασης (Broken Access Control) 613

21.2.5. Λανθασμένη παραμετροποίηση ασφάλειας (Security Misconfigurations) 616

21.2.6. Cross-Site Scripting (XSS) 616

21.2.7. Ανασφαλής αποσειριοποίηση αντικειμένων (Insecure Object Deserialization) 618

21.3. Τυποποιημένοι Μηχανισμοί Άμυνας 618

21.3.1. Πολιτική Ιδίας Προέλευσης (Same-Origin Policy) 618

21.3.2. Κεφαλίδες Ασφάλειας HTTP 620

21.3.3. Cookies 623

21.4. Ιδιωτικότητα στο Διαδίκτυο - Web Privacy 624

21.4.1. Διαδικτυακή παρακολούθηση - Web Tracking 625

21.4.2. Υπηρεσίες παρακολούθησης τοποθεσίας - Location tracking. 626

21.4.3. Κλοπή Δεδομένων - Data Theft 627

21.4.4. Ηλεκτρονικό ψάρεμα - Phishing attack.. 628

21.4.5. Στοχευμένο ηλεκτρονικό ψάρεμα - Spear phishing attack. 628

21.5. Σύνοψη 628

Βιβλιογραφικές αναφορές 629

ΜΕΡΟΣ Δ - Ασφάλεια Υποδομών 631

Κεφάλαιο 22 – Ασφάλεια Κρίσιμων Υποδομών 633

22.1. Εισαγωγή 634

22.2. Εννοιολογική Θεμελίωση 635

22.3. Είδη Κρίσιμων Υποδομών και Φορέων 636

22.3.1. Τομείς και κατηγορίες 636
22.3.2. Κριτήρια αξιολόγησης κρισιμότητας 637
22.3.3. Πλαίσια και κανονισμοί προστασίας κρίσιμων υποδομών 638

22.4. Μεθοδολογίες ασφάλειας στις Κρίσιμες Υποδομές 639

22.4.1. Κριτήρια αξιολόγησης μεθοδολογιών 640
22.4.2. Τεχνικές μοντελοποίησης μεθοδολογιών. 641

22.5. Αποτίμηση και Διαχείριση Επικινδυνότητας Κρίσιμων Υποδομών 642

22.5.1. Ιδιαιτερότητες Διαχείρισης Επικινδυνότητας των ΚΥ και ΦΕΒΥ 642
22.5.2. Σχέδια διαχείρισης επικινδυνότητας κρίσιμων υποδομών 644
22.5.3. Απειλές και ευπάθειες στις κρίσιμες υποδομές 646
22.5.4. Αποτίμηση Επιπτώσεων 647

22.6. Αλληλεξαρτήσεις κρίσιμων υποδομών και φορέων 648

22.7. SCADA και Βιομηχανικά Συστήματα Ελέγχου 651

22.7.1. Βασική αρχιτεκτονική 651
22.7.2. Επιθέσεις και ευπάθειες 652

22.8. Διαχείριση Επικινδυνότητας στις Κρίσιμες Υποδομές 655

22.8.1. Σύστημα διαχείρισης ασφάλειας πληροφοριών 655
22.8.2. Προγράμματα ελέγχων ασφάλειας 656
22.8.3. Βασικές ομάδες μέτρων προστασίας κρίσιμων υποδομών 657

22.9. Σύνοψη 658

Βιβλιογραφικές Αναφορές 659

Κεφάλαιο 23 – Ασφάλεια στο Δίκτυο..... 663

23.1. Εισαγωγή 664

23.2. Ασφάλεια στο επίπεδο μεταφοράς 665

23.2.1. Secure Shell (SSH) 665
23.2.2. Transport Layer Security (TLS) 675

23.3. Ασφάλεια στο επίπεδο δικτύου 689

23.3.1. Γενική Αρχιτεκτονική του IPSec 690
23.3.2. Συσχετίσεις Ασφαλείας 691
23.3.3. Μηχανισμός Αυθεντικοποίησης Επικεφαλίδας 693
23.3.4. Μηχανισμός Ασφαλούς Ενθυλάκωσης Ωφέλιμου Φορτίου (ESP) 695
23.3.5. Καταστάσεις λειτουργίας IPSec 696
23.3.6. Διαχείριση Κλειδιών στο IPSec 698

23.4. Σύνοψη 699

Βιβλιογραφικές Αναφορές 700

Κεφάλαιο 24 – Ασφάλεια στο Υλικό 703

24.1. Εισαγωγή 704

24.2. Ασφάλεια σε Intellectual Property Σχεδιασμούς 705

24.2.1. Επαναχρησιμοποίηση Σχεδιασμών 705
24.2.2. Η Έννοια του Intellectual Property Σχεδιασμού 706
24.2.3. Λόγοι Προστασίας Intellectual Property σχεδιασμού 706
24.2.4. Τρόποι Προστασίας Intellectual Property Σχεδιασμών 707
24.2.5. Υδατογράφηση Βασισμένη σε Περιορισμούς, για Προστασία Intellectual Property Σχεδιασμών 708

24.3. Δούρειοι Ίπποι (Trojan Horses) και Τεχνικές Ανίχνευσής τους ..709

24.3.1. Εισαγωγή στους Δούρειους Ίππους 709
24.3.2. Ανίχνευση Δούρειων Ίππων σε Ολοκληρωμένα Κυκλώματα 711

24.4. Φυσικές Μη Κλωνοποιήσιμες Συναρτήσεις (Physical Un-clonable Functions - PUFs) 714

24.4.1. Κατηγορίες Φυσικών Μη Κλωνοποιήσιμων Συναρτήσεων 715

24.4.2. Φυσικές Μη Κλωνοποιήσιμες Συναρτήσεις βασιζόμενες στην καθυστέρηση (Delay-based PUFs) 716

24.5. Επιθέσεις στο Υλικό 720

24.5.1. Αιτίες Επιθέσεων 720

24.5.2. Επίπεδα Ασφάλειας 721

24.5.3. Κατηγορίες Επιθέσεων 723

24.6. Σχεδιασμός, Υλοποίηση και Έλεγχος σε FPGAs 724

24.6.1. Μεθοδολογία Σχεδιασμού και Υλοποίησης 724

24.6.2. Έλεγχος 726

24.7. Σύνοψη 728

Βιβλιογραφικές Αναφορές 728

Κεφάλαιο 25 – Ασφάλεια Κυβερνο-Φυσικών Συστημάτων 731

25.1. Εισαγωγή 732

25.2. Ιδιάζοντα χαρακτηριστικά των ΚΦΣ 735

25.2.1. Υπολογιστική ισχύς 735

25.2.2. Λειτουργία πραγματικού χρόνου 735

25.2.3. Πρωτόκολλα επικοινωνίας 735

25.2.4. Έλεγχος 736

25.3. Προστασία ΚΦΣ έναντι φυσικών κινδύνων 737

25.3.1. Φυσική ασφάλεια και προστασία 737

25.3.2. Αξιοπιστία 739

25.3.3. Ανοχή σε σφάλματα 739

25.3.4. Εύρωστος έλεγχος 739

25.3.5. Φυσική ασφάλεια και κυβερνο-ασφάλεια 740

25.4. Επιθέσεις κατά της ασφάλειας των ΚΦΣ και της ιδιωτικότητας των χρηστών τους 741

25.4.1. Τύποι επιθέσεων κατά ΚΦΣ 741

25.4.2. Μερικές χαρακτηριστικές επιθέσεις 744

25.5. Προσεγγίσεις ασφάλειας ΚΦΣ 747

25.5.1. Πρόληψη επιθέσεων 747
25.5.2. Ανίχνευση επιθέσεων 751
25.5.3. Άμβλυνση των επιπτώσεων των επιθέσεων 755
25.6. Οι πολιτικές διαστάσεις της ασφάλειας ΚΦΣ 759
25.6.1. Κίνητρα και ρύθμιση 759
25.6.2. Κυβερνο-σύρραξη 761
25.7. Βιομηχανικές πρακτικές και πρότυπα ασφάλειας ΚΦΣ 764
25.8. Σύνοψη 765
Βιβλιογραφικές Αναφορές 766

Αντιστοίχιση Ελληνικών – Αγγλικών Όρων 777

Αντιστοίχιση Αγγλικών – Ελληνικών Όρων 795