Ασφάλεια Πληροφορίας και Συστημάτων

Σκοπός μαθήματος

Το μάθημα καλύπτει το γενικό μέρος της Ασφάλειας της Πληροφορίας και των Συστημάτων. Σκοπός του μαθήματος είναι η δημιουργία ενός βασικού πλαισίου θεωρητικών και εφαρμοσμένων γνώσεων στην ευρύτερη περιοχή της Ασφάλειας Πληροφοριακών και Επικοινωνιακών Συστημάτων σε δύο άξονες, την πληροφορία και το σύστημα. Το πλαίσιο αυτό θα συμπληρώσει επαρκώς το προφίλ του φοιτητή που ολοκληρώνει το μεταπτυχιακό αυτό κύκλο σπουδών στην Πληροφορική και θα αποτελέσει γι' αυτόν σημαντικό εφόδιο στην αγορά εργασίας.

Στόχοι μαθήματος

Με την επιτυχή ολοκλήρωση του μαθήματος αυτού, ο μεταπτυχιακός φοιτητής:

- θα γνωρίζει τα προβλήματα ασφάλειας σε Πληροφοριακά και Επικοινωνιακά Συστήματα,
- θα αναγνωρίζει τις ευπάθειες των πληροφοριακών και επικοινωνιακών συστημάτων,
- θα είναι σε θέση να εφαρμόσει βασικές αρχές σχεδιασμού πολιτικών ασφαλείας,
- θα γνωρίζει τα χαρακτηριστικά και τους μηχανισμούς ασφαλείας που υλοποιούν τις πολιτικές αυτές,
- θα έχει εξοικειωθεί με παραδείγματα που υλοποιούν και εφαρμόζουν μηχανισμούς ασφάλειας σε διαφορετικά Λειτουργικά Συστήματα,
- θα έχει γνώσεις στην περιοχή της Ασφάλειας Βάσεων Δεδομένων,
- θα γνωρίζει τα διαφορετικά είδη firewalls και πώς αυτά χρησιμοποιούνται και εφαρμόζονται,
- Θα γνωρίζει μηχανισμούς αυθεντικοποίησης, το ρόλο και τη σπουδαιότητά τους,
- Θα έχει εξοικειωθεί με τα Computer Forensics και θα έχει γνώση των εργαλείων που τα υποστηρίζουν,
- Θα γνωρίζει στοιχεία κρυπτογραφίας και κρυπτανάλυσης σε συμμετρικούς και ασύμμετρους κρυπτογραφικούς αλγόριθμους,
- και τέλος, θα έχει κατανοήσει τα Συστήματα Ανίχνευσης Εισβολών, τον τρόπο λειτουργίας τους και τις τεχνικές που χρησιμοποιούνται στις μηχανές ανίχνευσης αυτών.

Περιγραφή μαθήματος

Το μάθημα καλύπτει γενικά θέματα Ασφάλειας Πληροφορίας και Συστημάτων. Το περίγραμμα του μαθήματος περιλαμβάνει θεμελιώδεις έννοιες και ορολογία στην Ασφάλεια Πληροφορίας και Συστημάτων, θέματα κλασικής και ασφαλούς Κρυπτογράφησης (ασύμμετρης: RSA), ανεκτικότητα κρυπτογραφικών αλγόριθμων, προστασία Λειτουργικών

Συστημάτων, ασφάλεια Βάσεων Δεδομένων, Έλεγχο Πρόσβασης, ασφάλεια Δικτύων και Κατανεμημένων Συστημάτων, Ανίχνευση Επιθέσεων, Ανάλυση Επικινδυνότητας, Computer Forensics.

Περίγραμμα μαθήματος

1. Εννοιολογική θεμελίωση της Ασφάλειας Πληροφορίας και Συστημάτων
2. Κλασική Κρυπτογραφία
3. Ανεκτικότητα Συμμετρικών Κρυπτογραφικών Αλγορίθμων
4. Ασύμμετρη Κρυπτογραφία και Ψηφιακές Υπογραφές
5. Προστασία Λειτουργικών Συστημάτων, Αυθεντικοποίηση και Έλεγχος Πρόσβασης
6. Ασφάλεια Βάσεων Δεδομένων
7. Ασφάλεια Δικτύων Υπολογιστών και Κατανεμημένων Συστημάτων
8. Ανίχνευση Εισβολών
9. Computer Forensics
10. Ανάλυση Επικινδυνότητας

Συνιστώμενη Βιβλιογραφία

1. Stallings William και Brown Lawrie, Ασφάλεια Υπολογιστών – Αρχές και Πρακτικές, 3/Ε, 2016, Εκδόσεις ΚΛΕΙΔΑΡΙΘΜΟΣ.
2. Stallings William, Κρυπτογραφία και Ασφάλεια Δικτύων: Αρχές και Εφαρμογές, 5/Ε, 2012, Εκδοτικός Όμιλος Ίων.
3. Γκρίτζαλης Σ., Κάτσικας Σ., Γκρίτζαλης Δ., Ασφάλεια Δικτύων Υπολογιστών, Παπασωτηρίου, 2003.
4. Κάτσικας Σ.Κ., Γκρίτζαλης Δ., Γκρίτζαλης Σ., Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, 2004.
5. Bishop M., Computer Security – Art and Science, Addison-Wesley,2003.
6. Bishop M., Introduction to Computer Security, Addison-Wesley,2005.
7. Buchmann J., Introduction to Cyptography, 2nd Ed., Springer,2004.
8. Casey E., Handbook of Computer Crime Investigation – Forensic Tools and Technology, Academic Press, 2002.
9. Fourouzan B., "Cryptography and Network Security", 2008, Mc Graw-Hill.
10. Menezes A., Van Oorschot P., Vanstone S., Handbook of Applied Cryptography, HAC (free).
11. Mitnick K.D., Simon W.L., The Art of Deception, John Wiley & Sons, 2002.
12. Oppliger R., Security Technologies for the World Wide Web, Artech House Inc., 2000.
13. Pfleeger C.P., Lawrence Pfleeger S., Security in Computing, Prentice Hall, 2003.
14. Pieprzyk J., Hardjono T., Seberry J., Fundamentals of Computer Security, Springer, 2003.
15. Proctor P.E., The Practical Intrusion Detection Handbook, Prentice Hall, 2001.
16. Riggs G., Network Perimeter Security – Building Defense In-Depth, Auerbach, 2004.
17. Schultz E.E., Shumway R., Incident Response – A Strategic Guide to Handling System and Network Security Breaches, New Riders Publishing, 2002.
18. Spitzner L., Honeypots – Tracking Hackers, Addison Wisley, 2003.

19. Stallings William, Cryptography and Network Security: Principles and Practice, 5/E (free), 2012, Prentice Hall.

20. Young S., Aitel D., The Hacker's Handbook – The Strategy behind Breaking into and Defending Networks, Auerbach, 2004.