ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

1. ΓΕΝΙΚΑ

ΣΧΟΛΗ	ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ		
ΤΜΗΜΑ	ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	*Προπτυχιακό*		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ		**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	**7ο**
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ**		
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ		**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Διαλέξεις		3	6
Εργαστηριακές Ασκήσεις		2	
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	Επιστημονικής Περιοχής, Ανάπτυξης Δεξιοτήτων (Υποχρεωτικό Μάθημα Ειδικής Υποδομής (ΜΕΥ))		
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ:			
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ:	Ελληνικά/Αγγλικά		
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Ναι στην Αγγλική		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	http://elearn.teikoz.gr/course/view.php?id=368		

2. ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Ο σκοπός του μαθήματος είναι η εξοικείωση των φοιτητών με τις θεμελιώδεις αρχές της Ασφάλειας Υπολογιστικών Συστημάτων και τα προβλήματα ασφάλειας των σύγχρονων υπολογιστικών συστημάτων και δικτύων, τους μηχανισμούς και τις τεχνολογίες προστασίας τους, καθώς και την πρακτική εξάσκηση τους σε εργαστηριακό περιβάλλον, με την υλοποίηση κρυπτογραφικών αλγορίθμων, την ανίχνευση ευπαθειών και εισβολών, την αποτροπή εισβολών, την εφαρμογή μέτρων προστασίας και την ανάπτυξη πολιτικών ασφάλειας.

Με την επιτυχή ολοκλήρωση του μαθήματος ο φοιτητής / τρια θα είναι σε θέση :

- Να γνωρίζει και να εξηγεί τις θεμελιώδεις έννοιες στην ασφάλεια υπολογιστικών συστημάτων και δικτύων
- Να γνωρίζει και να αναλύει τους κυριότερους κρυπτογραφικούς αλγόριθμους και βασικά χαρακτηριστικά υλοποίησής τους σε προγραμματιστικό περιβάλλον.
- Να διακρίνει και να αναλύει τα βασικά χαρακτηριστικά ασφάλειας δικτύων και δικτυακών εφαρμογών, τις ιδιαίτερες ευπάθειες και απειλές που υφίστανται.
- Να γνωρίζει και να εφαρμόζει τους μηχανισμούς ασφάλειας και τα αντίστοιχα πρωτόκολλα σε όλα τα επίπεδα του TCP/IP και τους μηχανισμούς περιμετρικής άμυνας δικτύων.
- Να εξετάζει και να αξιολογεί τις ευπάθειες, τις απειλές και την εκτίμηση επικινδυνότητας σε ένα υπολογιστικό σύστημα.
- Να συγκρίνει και να αξιολογεί τα θεμελιώδη μοντέλα και πολιτικές ελέγχου πρόσβασης και να είναι σε θέση να αναπτύξει μια κατάλληλη πολιτική ασφάλειας και τους απαραίτητους μηχανισμούς ασφαλείας που θα την υποστηρίξουν.

Γενικές Ικανότητες

- Προσαρμογή σε νέες καταστάσεις

- Αυτόνομη Εργασία
- Σχεδιασμός και Διαχείριση Έργων
- Άσκηση κριτικής και αυτοκριτικής
- Προαγωγή της ελεύθερης, δημιουργικής και επαγωγικής σκέψης

3. ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Το περιεχόμενο του μαθήματος καλύπτει τα ακόλουθα θέματα:

ΕΙΣΑΓΩΓΗ

- Βασικές Αρχές Ασφάλειας
  Τάσεις στο χώρο της ασφάλειας, Η αρχιτεκτονική ασφάλειας OSI, Επιθέσεις ασφάλειας, Υπηρεσίες ασφάλειας, Μηχανισμοί ασφάλειας, Μοντέλο ασφάλειας δικτύων

ΜΕΡΟΣ ΠΡΩΤΟ - ΚΡΥΠΤΟΓΡΑΦΙΑ

- Συμμετρική κρυπτογράφηση
  Αρχές της συμμετρικής κρυπτογράφησης, Τεχνικές της συμμετρικής κρυπτογράφησης, Συμμετρικοί αλγόριθμοι κρυπτογράφησης τμημάτων, Τρόποι λειτουργίας κωδικοποιητών τμημάτων, Κωδικοποιητές Ροής, Εμπιστευτικότητα με χρήση συμμετρικής κρυπτογράφησης, Τοποθέτηση συσκευών κρυπτογράφησης, Κέντρο Διανομής κλειδιών
- Κρυπτογραφία δημόσιου κλειδιού και πιστοποίηση αυθεντικότητας μηνυμάτων
  Πιστοποίηση αυθεντικότητας μηνυμάτων, Ασφαλείς συναρτήσεις και αλγόριθμοι κατακερματισμού, Αρχές κρυπτογραφίας δημόσιου κλειδιού, Αλγόριθμοι κρυπτογραφίας δημόσιου κλειδιού, Ψηφιακές υπογραφές, Διαχείριση κλειδιών

ΜΕΡΟΣ ΔΕΥΤΕΡΟ – ΕΦΑΡΜΟΓΕΣ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ

- Εφαρμογές πιστοποίησης αυθεντικότητας
  Kerberos , Υπηρεσία πιστοποίησης X.509, Υποδομή δημόσιου κλειδιού
- Ασφάλεια ηλεκτρονικού ταχυδρομείου
- Pretty Good Privacy (PGP), S/MIME
- Ασφάλεια Πρωτοκόλλου IP (IPSec)
  Επισκόπηση του IPSec, Αρχιτεκτονική IPSec, Κεφαλίδα πιστοποίησης AH, Ενθυλάκωση φορτίου ασφάλειας ESP, Συνδυασμός συσχετίσεων ασφάλειας, Διαχείριση κλειδιών
- Ασφάλεια στον Παγκόσμιο Ιστό
  Θέματα ασφάλειας Παγκόσμιου Ιστού, Πρωτόκολλα SSL και TLS, Ασφαλής ηλεκτρονική συναλλαγή

ΜΕΡΟΣ ΤΡΙΤΟ – ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

- Εισβολείς
  Τεχνικές εισβολής, Ανίχνευση εισβολών (IDS), Αποτροπή εισβολών (IPS), Διαχείριση συνθηματικών
- Κακόβουλο λογισμικό
  Ιοί και συναφείς απειλές, Μέτρα αντιμετώπισης κακόβουλου λογισμικού, Κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDos)
- Τείχη Προστασίας
  Αρχές σχεδίασης Τειχών Προστασίας, Έμπιστα συστήματα
- Κριτήρια αξιολόγησης ασφάλειας στην τεχνολογία της πληροφορικής
  Απαιτήσεις λειτουργικότητας ασφάλειας, Απαιτήσεις εγγύησης ασφάλειας, Προφίλ προστασίας, Στόχοι ασφάλειας, Νομικά θέματα ασφάλειας (Computer Forensics).

Στο εργαστηριακό μέρος του μαθήματος οι φοιτητές έχουν τη δυνατότητα της πρακτικής εφαρμογής των εννοιών της θεωρίας με τη χρήση πλήθους ασκήσεων που καλύπτουν εκτενώς την ύλη, και να αποκτήσουν εμπειρία σχετικά με την χρήση μηχανισμών κρυπτογράφησης, αυθεντικοποίησης κι ελέγχου πρόσβασης, εφαρμογών ελέγχου ασφάλειας δικτύων και υπολογιστικών συστημάτων, χρησιμοποιώντας αντίστοιχα εργαλεία και βιβλιοθήκες λογισμικού (ανιχνευτές τρωτότητας, εργαλεία ελέγχου διείσδυσης κι εκμετάλλευσης ευπαθειών των υπολογιστικών συστημάτων, συστήματα ανίχνευσης εισβολέων και αποτροπής τους, τείχη προστασίας, κ.α).

4. ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ.	Διδασκαλία καθ΄ έδρας με τη χρήση οπτικοακουστικών μέσων. Εργαστηριακές ασκήσεις - πρακτική εφαρμογή.
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ	Χρήση εξειδικευμένων λογισμικών. Υποστήριξη Μαθησιακής διαδικασίας μέσω της ηλεκτρονικής πλατφόρμας ασύγχρονης τηλεκπαίδευσης (e-class)
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ	

Δραστηριότητα	***Φόρτος Εργασίας Εξαμήνου***
Διαλέξεις	39
Εργαστηριακές Ασκήσεις	26
Μικρές ατομικές εργασίες	7
Αυτοτελής Μελέτη	78
Σύνολο Μαθήματος (25 ώρες φόρτου εργασίας ανά πιστωτική μονάδα)	***150***

ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ	I. Γραπτή τελική εξέταση (60%) στην ελληνική γλώσσα, που περιλαμβάνει: - Δοκιμασία πολλαπλής επιλογής - Ερωτήσεις Σύντομης Απάντησης, - Επίλυση Προβλημάτων - Συγκριτική αξιολόγηση στοιχείων θεωρίας II. Εργαστηριακή Εξέταση (40%) στην ελληνική γλώσσα, που περιλαμβάνει: - Επίλυση εργαστηριακών ασκήσεων

5. ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- "Κρυπτογραφία για Ασφάλεια Δικτύων: Αρχές και Εφαρμογές", William Stallings, Εκδόσεις ΙΩΝ, Αθήνα, 2012
- "Βασικές Αρχές Ασφάλειας Δικτύων: Εφαρμογές και πρότυπα", Τρίτη αμερικανική έκδοση, William Stallings, Εκδόσεις Κλειδάριθμος, Αθήνα, 2008
- "Ασφάλεια Πληροφοριακών Συστημάτων και Δικτύων", Γ.Πάγκαλος & Ι.Μαυρίδης, Εκδόσεις ΑΝΙΚΟΥΛΑ, Θεσσαλονίκη, 2002
- "Ασφάλεια Δικτύων Υπολογιστών: Τεχνολογίες και Υπηρεσίες σε περιβάλλοντα Ηλεκτρονικού Επιχειρείν & Ηλεκτρονικής Διακυβέρνησης ", Σ. Γκρίτζαλης , Σ. Κάτσικας , Δ. Γκρίτζαλης, Εκδόσεις Παπασωτηρίου, Αθήνα, 2003
- "Ασφάλεια της Πληροφορίας", Α. Σουρής, Δ. Πατσός, Ν. Γρηγοριάδης, Εκδόσεις Νέων Τεχνολογιών, Αθήνα, 2004
- "Ασφάλεια Δικτύων", S. McClure, .J. Scambray, G. Kurtz, Εκδόσεις Γκιούρδας, Αθήνα, 2009