1. Ταυτότητα Μαθήματος

Κωδικός Μαθήματος: 4601
Τίτλος Μαθήματος: Ασφάλεια Πληροφοριακών Συστημάτων
Τίτλος Μαθήματος στα Αγγλικά: Security on Information Systems
Τύπος Μαθήματος: Μάθημα υποχρεωτικό, Μεικτό
Ώρες διδασκαλίας: 6 (4Θ+2Ε), Θεωρία: Τετάρτη 2-4 (109), Πέμπτη 11-1 (102)
Εξάμηνο: ΣΤ΄
Μονάδες ECTS: 6
Διδάσκοντες Θεωρία: Χρήστος Ηλιούδης, iliou@it.teithe.gr
Εργαστήριο: Χ. Ηλιούδης, iliou@it.teithe.gr, Δημ. Αμανατιάδης dima@it.teithe.gr
Ώρες Γραφείου: Τρίτη 1-2, Πέμπτη 1-2
Σελίδα μαθήματος: www.it.teithe.gr/~iliou/cs4601,

2. Μαθησιακοί στόχοι του μαθήματος:

Σκοπός του μαθήματος είναι οι φοιτητές να γνωρίζουν τα προβλήματα ασφάλειας των πληροφοριακών συστημάτων, τους μηχανισμούς και τις τεχνολογίες προστασίας τους, και να εκπαιδευτούν σε εργαστηριακό περιβάλλον στον προσδιορισμό ευπαθειών, στην ανάπτυξη πολιτικών ασφάλειας, στην εφαρμογή μέτρων προστασίας, καθώς και στην υλοποίηση κρυπτογραφικών αλγορίθμων.
Αναμένεται οι σπουδαστές με την ολοκλήρωση του μαθήματος (θεωρητικού και εργαστηριακού μέρους) να είναι σε θέση να γνωρίζουν:

- Τις θεμελιώδεις έννοιες στην ασφάλεια πληροφοριακών συστημάτων
- Τις ευπάθειες, τις απειλές και την εκτίμηση επικινδυνότητας σε ένα Πληροφοριακό σύστημα.
- Τα θεμελιώδη μοντέλα και πολιτικές ελέγχου πρόσβασης και να είναι σε θέση να αναπτύξουν μια κατάλληλη πολιτική ασφάλειας και τους απαραίτητους μηχανισμούς προστασίας που θα την υποστηρίξουν.
- Τους κυριότερους κρυπτογραφικούς αλγόριθμους και βασικά χαρακτηριστικά υλοποίησής τους σε προγραμματιστικό περιβάλλον.
- Τα βασικά χαρακτηριστικά ασφάλειας δικτύων και δικτυακών εφαρμογών, τις ιδιαίτερες ευπάθειες και απειλές που υφίστανται.
- Τους μηχανισμούς ασφάλειας και τα πρωτόκολλα εφαρμογής σε όλα τα επίπεδα του TCP/IP και τους μηχανισμούς περιμετρικής άμυνας δικτύων.
- Web security

3. Αντικείμενο του μαθήματος:

Τα θέματα που καλύπτει το θεωρητικό μέρος είναι:

- *Εννοιολογική Θεμελίωση*: βασικές έννοιες και ορισμοί στην ασφάλεια Πληροφοριακών Συστημάτων.
- *Ανάλυση και Διαχείριση Επικινδυνότητας:* δυνατότητες και περιορισμοί των τεχνικών ανάλυσης και διαχείρισης επικινδυνότητας

- *Μοντέλα και πολιτικές ελέγχου πρόσβασης*: Lattice, Bell-La Padula, MAC, DAC, RBAC
- *Στοιχεία κρυπτογραφίας*: κρυπταλγόριθμοι τμήματος και ροής κρυπτογραφία Δημοσίου κλειδιού, κρυπτογραφικές συναρτήσεις σύνοψης, κρυπτανάλυση.
- *Αυθεντικοποίηση Οντοτήτων:* Πρωτόκολλα και Τεχνολογίες αυθεντικοποίησης, Έξυπνες κάρτες, Βιομετρία, Ψηφιακά πιστοποιητικά, Ψηφιακή Υπογραφή, Υποδομή Δημοσίου Κλειδιού.
- *Ιομορφικό λογισμικό:* Μοντέλα και κατηγορίες κακόβουλου λογισμικού
- *Ασφάλεια Βάσεων Δεδομένων:* βασικές έννοιες, μοντέλα και πολιτικές ελέγχου πρόσβασης ΒΔ και μεθοδολογικό πλαίσιο σχεδιασμού ασφαλών ΒΔ.
- *Μοντέλα Ασφάλειας κινητού κώδικα*: Το μοντέλο ασφάλειας της Java και οι δυνατότητες υλοποίησης μηχανισμών ασφάλειας και κρυπταλγορίθμων.
- *Ασφάλεια στο Διαδίκτυο:* Απειλές και ευπάθειες, μηχανισμοί και πρωτόκολλα ασφάλειας δικτύου στα επίπεδα του TCP/IP.
- *Περιμετρική άμυνα δικτύου και ασφαλή διαχείρισή του*: Firewalls
- Web security (SQL Injections, XSS)

Στο εργαστηριακό μέρος του μαθήματος οι φοιτητές μελετούν και εκπαιδεύονται, ως συνέχεια του θεωρητικού μέρους, στα παρακάτω θέματα:

- *Εκτίμηση επικινδυνότητας ασφάλειας πληροφοριακού συστήματος:* Χρήση λογισμικού ανάλυσης κινδύνων Πληροφοριακών συστημάτων και ανάπτυξη ενός προσαρμοσμένου πλαισίου εκτίμησης επικινδυνότητας.
- *Σχεδιασμό πολιτικής ασφάλειας:* Μελέτη περίπτωσης, δημιουργία πολιτικής ασφάλειας
- *Έλεγχος ανθεκτικότητας και παραβίασης μηχανισμών αυθεντικοποίησης*: Μέθοδοι παραβίασης και μέτρα ισχυροποίησης
- *Ανάπτυξη και υλοποίηση κρυπτογραφικών αλγορίθμων:* Συμμετρικού (π.χ 3DES), δημοσίου κλειδιού (RSA), και σύνοψης (MD5, SHA)
- *Δημιουργία και επαλήθευση ψηφιακής υπογραφής:* Αλγόριθμος DSA, δημιουργία κλειδιών, υπογραφής και επαλήθευσης.
- *Προσδιορισμών ευπαθειών δικτύων:* Port Scanning, Sniffing, Spoofing.
- *Περιμετρική άμυνα - Firewalls:* Δημιουργία πολιτικής ασφάλειας σε firewall
- *Επιθέσεις Κοινωνικής μηχανικής*: Χρήση κατάλληλου λογισμικού και τεχνικών για τη δημιουργία επιθέσεων κοινωνικής μηχανικής (κλώνων κλπ)
- *Τεχνολογίες Προστασίας Ιδιωτικότητας και Τεχνολογίες ελέγχου Προσπέλασης στον παγκόσμιο ιστό με βάση το περιεχόμενο:* μελέτη των προτύπων RSAC, ICRA και μηχανισμών εφαρμογής τους.
- *Web security*: SQL Injections, XSS

4. Διδακτική Μέθοδος

Στο θεωρητικό μέρος η εκπαίδευση των φοιτητών στηρίζεται σε διαλέξεις, παρουσίαση και διερεύνηση επίκαιρων περιστατικών παραβιάσεων, χρήση υλικού πιστοποιημένων φορέων αντιμετώπισης παραβιάσεων ασφάλειας και παρουσίαση σχετικής βιβλιογραφίας για τα θέματα που αναπτύσσονται. Επιπλέον οι φοιτητές θα ερευνήσουν ένα ιδιαίτερο θέμα της ασφάλειας Πληροφοριακών συστημάτων το οποίο και θα παρουσιάσουν.
Στο εργαστηριακό μέρος του μαθήματος η εκπαίδευση στηρίζεται στη χρήση κατάλληλου λογισμικού ασφάλειας καθώς και στην υλοποίηση αλγορίθμων και μηχανισμών ασφάλειας.

5. Μέθοδος αξιολόγησης φοιτητών

Η αξιολόγηση των φοιτητών στο θεωρητικό μέρος στηρίζεται στην τελική γραπτή εξέταση, στην πρόοδο κατά τη διάρκεια του εκπαιδευτικού έτους, καθώς και στην τελική εργασία.
Η αξιολόγηση για το εργαστηριακό μέρος στηρίζεται στην τελική γραπτή εξέταση και στις εβδομαδιαίες ασκήσεις που παραδίδουν.

6. Χρόνος εκπλήρωσης του μαθήματος

Για το θεωρητικό μέρος:

Παρακολούθηση διδασκαλίας	Εργασία	Προσωπική Μελέτη	Σύνολο Ωρών
52	**[15]**	**40**	**92**

Για το εργαστηριακό μέρος:

Παρακολούθηση εργαστηρίου	Προσωπική Μελέτη	Ασκήσεις	Σύνολο Ωρών
26	**15**	**20**	**61**

7. Προαπαιτούμενες γνώσεις:

Αναμένεται πως κάθε φοιτητής γνωρίζει βασικές έννοιες Προγραμματισμού, Λειτουργικών Συστημάτων και Δικτύων, οι οποίες θα είναι χρήσιμες για ένα μέρος της ύλης.

8. Συγγράμματα / βιβλία

Ενδεικτικά αναφέρονται τα παρακάτω συγγράμματα που καλύπτουν τους μαθησιακούς στόχους του μαθήματος:

1. «Ασφάλεια Δικτύων Υπολογιστών», Σ. Γκρίτζαλης, Σ. Κάτσικας, Δ. Γκρίτζαλης,, εκδόσεις Παπασωτηρίου, 2003
2. «Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα» Κ. Λαμπρινουδάκης, Λ. Μήτρου, Σ. Γκρίτζαλης, Σ. Κάτσικας. Εκδόσεις Παπασωτηρίου, Αθήνα, 2009.