

ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	Μηχανικών		
ΤΜΗΜΑ	Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	Προπτυχιακό		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	9.018	ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ	9 ^ο
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Ασφάλεια Δικτύων και Τηλεπικοινωνιών		
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ	ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ	
Διαλέξεις και Ασκήσεις	4	2.5	
Εργαστήριο	1	1.5	
ΣΥΝΟΛΟ	5	4	
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	Εμβάθυνσης / Εμπέδωσης γνώσεων ειδικότητας		
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ			
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ	Ελληνική		
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Όχι		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://eclass.hmu.gr/courses/ECE189/		

(2) ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα
<p>Το μάθημα εστιάζει σε θέματα Ασφάλειας Δικτύων Υπολογιστών και Τηλεπικοινωνιακών Συστημάτων, καθώς και στις τεχνολογίες προστασίας της ιδιωτικότητας. Η προσέγγιση βασίζεται στην αρχιτεκτονική δικτύων OSI και συγκεκριμένα στην αρχιτεκτονική ασφάλειας στο μοντέλο του Internet. Επιπλέον εξετάζονται θέματα κυβερνοσφάλειας και ασφάλειας των κινητών επικοινωνιών. Το μάθημα προσπαθεί να καλλιεργήσει κουλτούρα ασφάλειας σε δικτυακό περιβάλλον, παρουσιάζοντας τις διάφορες κατηγορίες απειλών, των σημείων ευπάθειας, των αντιμέτρων, και των μεθόδων διασφάλισης. Επιπλέον, επιδιώκει την εξοικείωση με τη σχετική ορολογία και τις βασικές τεχνολογίες προστασίας της ιδιωτικότητας.</p> <p>Με την επιτυχή ολοκλήρωση του μαθήματος ο φοιτητής / τρια θα είναι σε θέση να:</p> <ol style="list-style-type: none">1. Εξηγεί το ρόλο και τη σημασία της ασφάλειας τηλεπικοινωνιών και δικτύων2. Εφαρμόζει συμμετρικούς κρυπτογραφικούς αλγόριθμους και αλγόριθμους δημόσιου κλειδιού3. Αναλύει και αποτιμά συστήματα ασφάλειας τηλεπικοινωνιών και δικτύων4. Σχεδιάζει και υλοποιεί ασφαλή δικτυακά συστήματα και εφαρμογές5. Κρίνει τα πλεονεκτήματα και τα μειονεκτήματα εναλλακτικών αρχιτεκτονικών ασφάλειας6. Σχεδιάζει και υλοποιεί εφαρμογές blockchain
Γενικές Ικανότητες
<ul style="list-style-type: none">▪ Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών▪ Προσαρμογή σε νέες καταστάσεις▪ Αυτόνομη εργασία▪ Ομαδική εργασία▪ Εργασία σε διεπιστημονικό περιβάλλον▪ Παραγωγή νέων ερευνητικών ιδεών

(3) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

Ενότητες Θεωρητικών Διαλέξεων

- Εισαγωγικά θέματα Ασφάλειας Δικτύων Υπολογιστών: Κατηγορίες Απειλών, Σημεία Ευπάθειας, Αντίμετρα, Διασφάλιση.
- Ασφάλεια Επιπέδου Internet, Ασφάλεια Επιπέδου Μεταφοράς, Ασφάλεια Επιπέδου Εφαρμογής.
- Αναχώματα Ασφάλειας: Δυνατότητες και Περιορισμοί, Ζητήματα Σχεδίασης, Αρχιτεκτονική Αναχωμάτων Ασφάλειας, Αναχώματα Ασφάλειας Επιπέδου Δικτύου / Επιπέδου Εφαρμογής, Υβριδικά Αναχώματα Ασφάλειας.
- Συστήματα Ανίχνευσης Εισβολών.
- Ασφάλεια σε περιβάλλον ασύρματων και κινητών δικτύων επικοινωνιών (2/3/4 G, UMTS, IEEE 802.11 και 802.16).
- Κίνδυνοι και επισφάλειες από τη χρήση της νεφοϋπολογιστικής.
- Τεχνολογίες προστασίας της ιδιωτικότητας, ανωνυμία και ψευδωνυμία.
- Ασφάλεια δικτύων αισθητήρων και ενσωματωμένων συστημάτων.
- Κακόβουλο λογισμικό.
- Συμμετρική κρυπτογραφία και Κρυπτογραφία δημόσιου κλειδιού.
- Ψηφιακές υπογραφές και πιστοποιητικά.
- Ασφάλεια μέσω αρχιτεκτονικής blockchain.

Εργαστηριακές Ασκήσεις

Στο εργαστηριακό μέρος του μαθήματος οι φοιτητές έχουν τη δυνατότητα της πρακτικής εφαρμογής των εννοιών της θεωρίας με τη χρήση ασκήσεων που καλύπτουν εκτενώς την ύλη, και να αποκτήσουν εμπειρία σχετικά με την χρήση μηχανισμών ασφάλειας σε δικτυακά περιβάλλοντα υπολογιστικών συστημάτων, χρησιμοποιώντας αντίστοιχα εργαλεία και βιβλιοθήκες λογισμικού.

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ	Πρόσωπο με πρόσωπο στην τάξη	
ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ	Χρήση Τ.Π.Ε. στη διδασκαλία Χρήση Τ.Π.Ε. στην εργαστηριακή εκπαίδευση Χρήση Τ.Π.Ε. στην επικοινωνία με τους φοιτητές μέσω της ηλεκτρονικής πλατφόρμας e-class	
ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ	Δραστηριότητα	Φόρτος Εργασίας Εξαμήνου
	Διαλέξεις	52
	Εργαστηριακή Άσκηση	13
	Αυτοτελής μελέτη	17
	Ομαδική εργασία Θεωρίας	10
	Ομαδική εργασία Εργαστηρίου	15
	Εβδομαδιαίες ασκήσεις για το σπίτι	13
	Σύνολο Μαθήματος	120
ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ	Μέθοδοι αξιολόγησης: 1. Γραπτή τελική εξέταση (40%) <ul style="list-style-type: none">▪ με επίλυση προβλημάτων▪ με ερωτήσεις πολλαπλής επιλογής 2. Ομαδική εργασία θεωρίας (αναφορά και προφορική εξέταση) (20%)	

	<p>3. Ομαδική εργασία εργαστηρίου (αναφορά και προφορική εξέταση) (30%)</p> <p>4. Εβδομαδιαίες ασκήσεις για το σπίτι (10%)</p> <p>Τα κριτήρια αξιολόγησης ανακοινώνονται στους φοιτητές κατά την έναρξη του εξαμήνου και βρίσκονται αναρτημένα στην ιστοσελίδα του μαθήματος στο eClass.</p>
--	--

(5) ΣΥΝΙΣΤΩΜΕΝΗ-ΒΙΒΛΙΟΓΡΑΦΙΑ

- Προτεινόμενη Βιβλιογραφία:

- Α. Πομπόρτσος & Γ. Παπαδημητρίου, "Ασφάλεια Δικτύων Υπολογιστών." Τζιόλας, 2002.
- Βασικές Αρχές Ασφάλειας Δικτύων: Εφαρμογές και Πρότυπα, William Stallings, έκδοση 3η, 2008 (μετάφραση).
- Ασφάλεια υπολογιστών: Αρχές και πρακτικές, William Stallings, Lawrie Brown, 3η έκδοση, 2016 (μετάφραση).
- Σ. Γκριτζαλης, Σ. Κάτσικας, Δ. Γκριτζαλης, Ασφάλεια Δικτύων Υπολογιστών, Εκδόσεις Παπασωτηρίου, 2004.
- W. Stallings, L. Brown, Ασφάλεια Υπολογιστών: Αρχές και Πρακτικές, Έκδοση 3η Αμερικανική, ISBN 978-960-461-668-8, Εκδόσεις Κλειδάριθμος, 2016.
- Λαμπρινουδάκης, Κ., Μήτρου, Λ., Γκριτζαλης, Σ., Κάτσικας, Σ., (Eds.), Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών: Τεχνικά και Νομικά Θέματα, Παπασωτηρίου, 2009.
- OWASP Testing Guide v4.
- "Security Engineering" (2nd Edition), Ross Anderson, Wiley (2008), ISBN: 0470068523
- "Principles of Computer Security, CompTIA Security+", Arthur Conklin and Gregory White, McGraw Hill (2012), ISBN: 9780071786164
- "Hacking Exposed 7: Network Security Secrets & Solutions" (7th Edition), Stuart McClure, Joel Scambray, George Kurtz, McGraw-Hill Osborne (2012)
- NIST Computer Security Resource Center, <http://csrc.nist.gov/>
- "Cryptography Engineering: Design Principles and Practical Applications", Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Wiley (2010), ISBN: 9780470474242

- Συναφή επιστημονικά περιοδικά:

- IEEE Communications Surveys and Tutorials
- IEEE Communications Magazine
- IEEE Journal on Selected Areas in Communications
- IEEE Network
- Elsevier Computer Networks
- IEEE Access
- Network Security - Journal – Elsevier
- International Journal of Network Security & Its Applications (IJNSA)
- Security and Communication Networks