ΠΕΡΙΓΡΑΜΜΑ ΜΑΘΗΜΑΤΟΣ

(1) ΓΕΝΙΚΑ

ΣΧΟΛΗ	Μηχανικών		
ΤΜΗΜΑ	Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	Προπτυχιακό (Πρώτος κύκλος σπουδών)		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	9.015	**ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ**	$9^{ο}$
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	Ασφάλεια Υπολογιστικών Συστημάτων		

ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
Θεωρητικές διαλέξεις	3	2
Ασκήσεις πράξης	1	1
Εργαστηριακές ασκήσεις	1	1
ΣΥΝΟΛΟ	**5**	**4**

ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	Εμβάθυνσης / Εμπέδωσης γνώσεων ειδικότητας
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ	Λειτουργικά Συστήματα
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ	Ελληνική
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Ναι
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://eclass.hmu.gr/courses/ECE150

(2) ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ

Μαθησιακά Αποτελέσματα

Σκοπός του μαθήματος είναι η κατανόηση του τρόπου λειτουργίας πολύ-επίπεδων μηχανισμών προστασίας ενός υπολογιστικού συστήματος με έμφαση σε ενσωματωμένα συστήματα (embedded system security).

Έμφαση δίνεται σε βασικούς μηχανισμούς και πρωτόκολλα που βασίζονται σε λογισμικό (βιβλιοθήκες κρυπτογραφίας) ή υλικό (programmable crypto engines, crypto ICs) υποστηρίζουν σε θέματα ελέγχου πρόσβασης, εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας, καθώς επίσης και στις τεχνικές με τις οποίες επεκτείνεται η χρήση τους σε υψηλό επίπεδο συστήματος (π.χ. file systems, memory) ή/ και εφαρμογής.

Με την επιτυχή ολοκλήρωση του μαθήματος οι φοιτητές θα είναι σε θέση:

- Να κατανοούν βασικές αρχές ασφάλειας της πληροφορίας και να συγκρίνουν πρωτόκολλα και τεχνικές security & data privacy σε επίπεδο device, network, system και application
- Να έχουν κατανοήσει σε βάθος την υποδομή συμμετρικών αλγορίθμων, δημοσίου κλειδιού και τη χρήση ψηφιακών πιστοποιητικών/υπογραφών καθώς και την χρήση τους για την υλοποίηση πολύπλοκων συστημάτων (Embedded Security, Cybersecurity)
- Να αποκτήσουν ευχέρεια στην αξιολόγηση του επιπέδου ασφάλειας, ανιχνεύοντας πιθανές εισβολές σε συσκευές, συστήματα και δίκτυα δεδομένων προσδιορίζοντας τα πιθανά threat models και να σχεδιάζουν και εφαρμόζουν μηχανισμούς πρόληψης κινδύνων (π.χ. hardware security, network firewalls, system/kernel security, least privileges, diversification)
- Να αναπτύσουν και υλοποιούν λύσεις ασφάλειας που ενοποιούν κρυπτογραφικές μεθόδους καθώς και μεθόδους απομόνωσης και ανωνυμίας για τη δημιουργία αποδοτικών μηχανισμών και βιβλιοθηκών θωράκισης (security patterns/libraries) σε επίπεδο device, network, system και εφαρμογής

Γενικές Ικανότητες

Το μάθημα αποσκοπεί στην απόκτηση, από τον πτυχιούχο, των παρακάτω γενικών ικανοτήτων:

- 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

Το μάθημα αποτελείται από σειρά διαλέξεων στις ενότητες.

- Ιστορική Αναδρομή - Αρχές – Κλασσική κρυπτογραφία - Μαθηματική Προσέγγιση
- Ασφάλεια Συστήματος – Linux Security – Domain Isolation = ARM Trustzone
- Κακόβουλο Λογισμικό (virus) - SW Vulnerabilities – Debugging/Reverse Engineering
- Side Channel Attacks – Energy Profiling
- Ασφάλεια Δικτύου – Worms –Virus – IPSec/TLS – DDoS – syslog/IDPS
- Υπηρεσίες Ασφάλειας – Προστασία Δεδομένων – Ανωνυμία
- Συμμετρική Κρυπτογραφία
- Κρυπτογραφία Δημόσιου Κλειδιού (RSA, Diffie Hellmann) & Ελλειπτική
- Ψηφιακά Πιστοποιητικά & Υπογραφές
- Πιστοποίηση Αυθεντικότητας Μηνυμάτων - Merkle Trees
- Embedded System Security, IoT Device Security, Cybersecurity & Safety, π.χ. Smart Vehicles
- Νομοθετικό/Ρυθμιστικό Πλαίσιο GDPR
- Programmable Crypto Engines – Crypto ICs – Software Libraries
- Cloud/IoT Security (Kerberos vs Auth)
- Ασφάλεια Εφαρμογών – Web/Ηλεκτρονικό Ταχυδρομείο (HTTPS, SMTP)
- Επιλεγμένα Θέματα (Κρυπτονομίσματα, Στεγανογραφία, Secret Sharing, zero-Knowledge Proofs, Homomorphic Security, Oblivious Transfer, Commit Protocols)

Εργαστηριακές Ασκήσεις

Στο εργαστηριακό μέρος του μαθήματος οι φοιτητές έχουν τη δυνατότητα πρακτικής εφαρμογής εννοιών της θεωρίας.

Στο εργαστηριακό μέρος του μαθήματος οι φοιτητές έχουν τη δυνατότητα να αποκτήσουν πρακτική εμπειρία στη χρήση κρυπτογραφικών μηχανισμών ασφάλειας υπολογιστικών συστημάτων χρησιμοποιώντας λογισμικό, εργαλεία, βιβλιοθήκες κρυπτογράφησης, programmable crypto engines, και crypto ICs κυρίως σε περιβάλλον Linux. Σκοπός είναι να αποκτήσουν εμπειρία σχετικά με την χρήση μηχανισμών κρυπτογράφησης (AES encryption/decryption), αυθεντικοποίησης (SHA3, one-way hash functions), απομόνωσης (domain isolation), και ανωνυμίας στην ανάπτυξη βιβλιοθηκών με security patterns και στην υλοποίηση ασφαλών πρωτοκόλλων διαχείρισης δεδομένων σε υψηλό επίπεδο για διάφορα συστήματα και εφαρμογές.

(4) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ - ΑΞΙΟΛΟΓΗΣΗ

<table>
<tr><td>ΤΡΟΠΟΣ ΠΑΡΑΔΟΣΗΣ</td><td>Πρόσωπο με πρόσωπο στην τάξη</td></tr>
<tr><td>ΧΡΗΣΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ</td><td>• 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</td></tr>
<tr><td>ΟΡΓΑΝΩΣΗ ΔΙΔΑΣΚΑΛΙΑΣ</td><td>
<table>
<tr><th>Δραστηριότητα</th><th>Φόρτος Εργασίας Εξαμήνου</th></tr>
<tr><td>Διαλέξεις</td><td>39</td></tr>
<tr><td>Demos/Ασκήσεις</td><td>26</td></tr>
<tr><td>Προσωπική Μελέτη & Προγρ/σμός (σε Server ή Laptop/PC μέσω VM)</td><td>55</td></tr>
<tr><td>Σύνολο Μαθήματος</td><td>120</td></tr>
</table>
</td></tr>
<tr><td>ΑΞΙΟΛΟΓΗΣΗ ΦΟΙΤΗΤΩΝ</td><td>Γλώσσα Αξιολόγησης: Ελληνική

Μέθοδοι αξιολόγησης:
1. Γραπτή τελική εξέταση σε θεωρητικά και κυρίως εργαστηριακά προβλήματα (50%)
2. Προγραμματιστικές εργασίες και προφορική εξέταση (50%)

Σε περιπτώσεις φοιτητών με αρκετή προγραμματιστική εμπειρία οι παραπάνω εξετάσεις και προγραμματιστικές εργασίες αντικαθίστανται από μεγάλη προγραμματιστική εργασία η οποία καλύπτει σε βάθος σημαντικές ενότητες του μαθήματος (π.χ. Cybersecurity, ή άλλαεπιλεγμένα θέματα). Σε αυτή την περίπτωση, στο τελευταίο εργαστηριακό μάθημα, γίνεται ανοικτή παρουσίαση και επίδειξη του συστήματος, εργαλείου, πλατφόρμας, ή εφαρμογής που θα υλοποιήσει ο φοιτητής.

Τα κριτήρια αξιολόγησης ανακοινώνονται στους φοιτητές κατά την έναρξη του εξαμήνου και βρίσκονται αναρτημένα στην ιστοσελίδα του μαθήματος στο eClass</td></tr>
</table>

(5) ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Προτεινόμενη Βιβλιογραφία:

- *P. C. Pfleeger, S. L. Pfleeger, J. Margulies, "Security in Computing", 5th edition, 2018. Prentice Hall, 2018.*
- *D. Basin, P. Schaller, M. Schlaepfer, "A Hands on Approach", Springer, 2011.*

Λοιπές πηγές:

- *Άρθρα από συναφή επιστημονικά περιοδικά και συνέδρια (στα Αγγλικά).*
- *Υποστήριξη Εργαστηρίου μέσω eclass με σημειώσεις, παραδείγματα με κώδικα και επεξηγήσεις.*
- *Στο εργαστήριο χρησιμοποιούνται διάφορα αναπτυξιακά boards, pirate devices, καθώς και virtual machines για την ασφαλή ανάπτυξη κώδικα/επιθέσεων, που συνοδεύονται από ανοικτού κώδικα ή licensed software και εγχειρίδια.*