1.8.5 Ασφάλεια Υλικού

(α) **ΓΕΝΙΚΑ**

ΣΧΟΛΗ	ΟΙΚΟΝΟΜΙΑΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ		
ΤΜΗΜΑ	ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ		
ΕΠΙΠΕΔΟ ΣΠΟΥΔΩΝ	ΠΡΟΠΤΥΧΙΑΚΟ		
ΚΩΔΙΚΟΣ ΜΑΘΗΜΑΤΟΣ	ΨΣΕ14		
ΕΞΑΜΗΝΟ ΣΠΟΥΔΩΝ	Η		
ΤΙΤΛΟΣ ΜΑΘΗΜΑΤΟΣ	**ΑΣΦΑΛΕΙΑ ΥΛΙΚΟΥ**		
ΑΥΤΟΤΕΛΕΙΣ ΔΙΔΑΚΤΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ		**ΕΒΔΟΜΑΔΙΑΙΕΣ ΩΡΕΣ ΔΙΔΑΣΚΑΛΙΑΣ**	**ΠΙΣΤΩΤΙΚΕΣ ΜΟΝΑΔΕΣ**
	Διαλέξεις	3	
	Φροντιστηριακή διδασκαλία	1	
	Σύνολο	4	6
ΤΥΠΟΣ ΜΑΘΗΜΑΤΟΣ	κατ' επιλογήν υποχρεωτικό, επιστημονικής περιοχής (ειδικού υποβάθρου), μάθημα με φροντιστήριο		
ΠΡΟΑΠΑΙΤΟΥΜΕΝΑ ΜΑΘΗΜΑΤΑ			
ΓΛΩΣΣΑ ΔΙΔΑΣΚΑΛΙΑΣ και ΕΞΕΤΑΣΕΩΝ	Ελληνική		
ΤΟ ΜΑΘΗΜΑ ΠΡΟΣΦΕΡΕΤΑΙ ΣΕ ΦΟΙΤΗΤΕΣ ERASMUS	Ναι (στην Αγγλική)		
ΗΛΕΚΤΡΟΝΙΚΗ ΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ (URL)	https://eclass.uop.gr/modules/auth/opencourses.php?fc=294		

(β) **ΜΑΘΗΣΙΑΚΑ ΑΠΟΤΕΛΕΣΜΑΤΑ**

Μαθησιακά Αποτελέσματα

Σκοπός του μαθήματος είναι παρουσίαση του αντικειμένου της Ασφάλειας Υλικού. Αρχικά γίνεται μια εισαγωγή στο αντικείμενο του μαθήματος και παρουσιάζονται παραδείγματα επιθέσεων καθώς και υλοποιήσεις οι οποίες είναι ευάλωτες. Παρουσιάζονται αναλυτικά υλοποιήσεις κρυπτογραφικών αλγορίθμων και επιθέσεις υλικού οι οποίες είναι σε θέση να εξάγουν πληροφορίες από αυτούς. Αναλύονται επιθέσεις εισαγωγής σφαλμάτων καθώς και επιθέσεις πλευρικού καναλιού. Στη συνέχεια παρουσιάζονται μεθοδολογίες υλοποίησης αντιμέτρων για την προστασία των αλγορίθμων από επιθέσεις υλικού. Γίνεται εισαγωγή στις Φυσικές μη Κλωνοποιήσιμες Συναρτήσεις (PUF) και στα Trojans Υλικού.

Μέσω της παρουσίασης διάφορων επιθέσεων και ευάλωτων υλοποιήσεων, οι φοιτητές θα μπορούν:

- να περιγράψουν και αναλύσουν κρυπτογραφικούς αλγόριθμους και επιθέσεις υλικού (επιθέσεις εισαγωγής σφαλμάτων, επιθέσεις πλευρικού καναλιού) με τις οποίες θα μπορούν να εξάγουν πληροφορίες από αυτούς,
- να χρησιμοποιούν μεθοδολογίες υλοποιήσεις αντιμέτρων για τη προστασία των αλγόριθμων από επιθέσεις υλικού,
- να υλοποιούν αξιολογήσεις ασφάλειας υλικού και να σχεδιάζουν αντίμετρα για

την προστασία ασφαλών υλοποιήσεων.

Ως αποτέλεσμα της επιτυχούς παρακολούθησης του μαθήματος, οι φοιτητές και φοιτήτριες θα έχουν εξοικειωθεί και αποκτήσει δεξιότητες στη χρήση αντίστοιχων τεχνολογιών.

Γενικές Ικανότητες

- Αυτόνομη εργασία
- Αναζήτηση, ανάλυση και σύνθεση δεδομένων και πληροφοριών, με τη χρήση και των απαραίτητων τεχνολογιών

(γ) ΠΕΡΙΕΧΟΜΕΝΟ ΜΑΘΗΜΑΤΟΣ

- Εισαγωγή στην ασφάλεια υλικού
- Ασφαλή ενσωματωμένα συστήματα (MCU/FPGA)
- Υλοποίηση του Advanced Encryption Standard (AES) σε FPGA και MCU
- Επιθέσεις εισαγωγής σφαλμάτων (Fault Injection Attacks)
- Δυσλειτουργίες τροφοδοσίας και Δυσλειτουργίες ρολογιού
- Επιθέσεις πλευρικού καναλιού (Side Channel Attacks)
- Ανάλυση κατανάλωσης και Ανάλυση ηλεκτρομαγνητικής ακτινοβολίας
- Αντίμετρα επιθέσεων υλικού (Hardware Attack Countermeasures)
- Πλεονασμός υλικού και χρονικός πλεονασμός για ανίχνευση σφαλμάτων
- Κώδικες ανίχνευσης σφαλμάτων
- Αντίμετρα απόκρυψης διαρροών πλευρικού καναλιού
- Φυσικές μη κλωνοποιήσιμες συναρτήσεις σε FPGA (Physically Unclonable Functions)
- Trojans υλικού (Hardware Trojans)

(δ) ΔΙΔΑΚΤΙΚΕΣ και ΜΑΘΗΣΙΑΚΕΣ ΜΕΘΟΔΟΙ – ΑΞΙΟΛΟΓΗΣΗ

Τρόπος Παράδοσης

Στην τάξη με χρήση διαφανειών, πίνακα και ηλεκτρονικού υπολογιστή για τη θεωρία καθώς και παραδείγματα και ασκήσεις του μαθήματος

Χρήση Τεχνολογιών Πληροφορικής και Επικοινωνιών

Υποστήριξη μαθησιακής διαδικασίας μέσω της ηλεκτρονικής πλατφόρμας e-class.

Οργάνωση Διδασκαλίας

Δραστηριότητα	Φόρτος Εργασίας Εξαμήνου

Διαλέξεις	39
Φροντιστηριακή διδασκαλία	13
Αυτοτελής μελέτη	98
Σύνολο μαθήματος	150

Αξιολόγηση Φοιτητών

Το μάθημα αξιολογείται με γραπτή τελική εξέταση τρίωρης διάρκειας, και πιθανή διαδικασία διαρκούς αξιολόγησης κατά την κρίση του διδάσκοντα. Η ακριβής διαδικασία αξιολόγησης ανακοινώνεται στους φοιτητές και αναρτάται στο eclass στην αρχή του εξαμήνου.

(ε) ΣΥΝΙΣΤΩΜΕΝΗ ΒΙΒΛΙΟΓΡΑΦΙΑ

Προτεινόμενη Βιβλιογραφία

1. B. Swarup, and M.Tehranipoor, ***Hardware security: a hands-on learning approach***, Morgan Kaufmann, 2018
2. Sakiyama, Kazuo, Yu Sasaki, and Yang Li, ***Security of block ciphers: from algorithm design to hardware implementation***, John Wiley and Sons, 2016

Συναφή Επιστημονικά Περιοδικά

1. IACR Transactions on Cryptographic Hardware and Embedded Systems
2. SPRINGER Journal of Hardware and Systems Security