Σ Ε Μ Ι Ν Α Ρ Ι Ο Τ Μ Η Μ Α Τ Ο Σ

ΟΜΙΛΗΤΗΣ: **Βασίλης Τενέντες**
Επίκουρος Καθηγητής
Τμήμα Μηχ. Η/Υ & Πληροφορικής
Πανεπιστήμιο Ιωαννίνων

ΗΜΕΡΟΜΗΝΙΑ: **Τετάρτη, 3 Απριλίου 2024**

ΩΡΑ: **12:00**

ΑΙΘΟΥΣΑ: **Αίθουσα Σεμιναρίων**

Θέμα

Σχεδίαση Υλικού για την Ασφάλεια Αναδυόμενων Εφαρμογών Υπολογιστικών Συστημάτων

Περίληψη

(Δυστυχώς) Το παγκόσμιο κλίμα γεωπολιτικής εσωστρέφειας έχει δημιουργήσει περισσότερες απαιτήσεις ασφάλειας, όπως είναι ο έλεγχος ακεραιότητας και η εμπιστευσιμότητα, όχι μόνο σε υπολογιστικά συστήματα υψηλού κόστους που χρησιμοποιούνται στην αμυντική βιομηχανία, στις μεταφορές, στην αεροδιαστημική και στις χρηματοπιστωτικές συναλλαγές, αλλά και σε υπολογιστικά συστήματα μεσαίου και χαμηλού κόστους που συνήθως συναντάμε σε προσωπικούς υπολογιστές, σε κινητά τηλέφωνα και σε εφαρμογές του διαδικτύου των πραγμάτων. Στην ομιλία αυτή θα παρουσιαστούν προσπάθειες που γίνονται ώστε οι απαιτήσεις αυτές να καλυφθούν μέσω ειδικών ολοκληρωμένων κυκλωμάτων, τα οποία υλοποιούν κρυπτογραφικές συναρτήσεις στο υλικό.

Συγκεκριμένα, θα παρουσιαστούν ενεργειακά αποδοτικοί σχεδιασμοί ψηφιακών κυκλωμάτων κρυπτογραφικών συναρτήσεων κατακερματισμού, βασισμένοι στον αλγόριθμο Secure Hash Algorithm 2 (SHA2), και ένας σχεδιασμός μιας ισχυρής μη-κλωνοποιήσιμης φυσικής συνάρτησης με χρήση υπολογιστικής σε SRAM μνήμη. Από τη μία, ο ενεργειακά αποδοτικός σχεδιασμός του SHA2 έχει εφαρμογές τόσο στον διαρκή έλεγχο της ακεραιότητας και στην ανίχνευση παραβιάσεων σε μηχανισμούς ασφαλούς πρόσβασης συσκευών, όσο και στα κατανεμημένα συστήματα διαρκούς ελέγχου ακεραιότητας συναλλαγών, όπως είναι τα δίκτυα αλυσίδων κοινοποιήσεων (Blockchain) και τα κρυπτονομίσματα. Από την άλλη, ο σχεδιασμός της μη-κλωνοποιήσιμης φυσικής συνάρτησης ενισχύει με χαμηλό κόστος την εμπιστευσιμότητα των υπολογιστικών συστημάτων, αφού επιτρέπει τη συλλογή στατικής εντροπίας από συστοιχίες SRAM κελιών τόσο για τη δημιουργία κρυπτογραφικών κλειδιών όσο και για τον έλεγχο ταυτότητας ολοκληρωμένων κυκλωμάτων.

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ Η/Υ & ΠΛΗΡΟΦΟΡΙΚΗΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
Τ.Θ. 1186, ΙΩΑΝΝΙΝΑ, 45110
Τ: 265100 8817 - 8813 - 7196
http://www.cse.uoi.gr

DEPT. OF COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF IOANNINA
P.O. BOX 1186, IOANNINA
GR-45110, GREECE
T: +30 265100 8817 - 8813 - 7196
http://www.cse.uoi.gr