Τμήμα Μηχανικών, Πληροφορικής & Τηλεπικοινωνιών, ΔΙΠΑΕ

Περιγραφή διδακτορικής διατριβής

Θέμα: Ανάπτυξη και επαλήθευση αλγοριθμικών τεχνικών ασφαλείας κυβερνοφυσικών συστημάτων

1. Τα αξιόπιστα περιβάλλοντα εκτέλεσης (Trusted Execution Environments – TEEs) ενθυλακομένων συστημάτων επιτρέπουν στις συσκευές να εκτελούν το λογισμικό τους σε έναν ασφαλή περιβάλλον-θύλακα (trusted enclaves), διασφαλίζοντας ταυτόχρονα την ακεραιότητα και την εμπιστευτικότητα των δεδομένων. Η ανάγκη για ανάλυση και επαλήθευση ασφαλείας των συστημάτων αυτών γίνεται επιτακτικότερη από το γεγονός ότι οι παραπάνω συσκευές αποτελούν βασικά δομικά στοιχεία υπολογιστικών συστημάτων στο νέφος ή/και κυβερνοφυσικών συστημάτων τα οποία βρίσκονται συνεχώς υπό καθεστώς επιθέσεων. Η παρούσα διδακτορική διατριβή θα ενασχοληθεί με την ανάπτυξη νέων αλγοριθμικών προσεγγίσεων ασφαλείας με υψηλό βαθμό ανεκτικότητας σε επιθέσεις (λ.χ. side channel attacks) και προχωρημένων κρυπτοαναλύσεων στην μετα-κβαντικής εποχής ασφάλεια (postquantum security); Όλες οι μέθοδοι θα πιστοποίηθούν με την βοήθεια τυπικών μεθόδων ανάλυσης και επαλήθευσης, ερευνώντας σε βάθος την ανθεκτικότητα των νέων περιβάλλοντων εκτέλεσης έναντι προηγμένων κακόβουλων επιθέσεων στο υλικό και στο λογισμικό της συσκευής.