ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ
ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

UNIVERSITY OF PIRAEUS
DEPARTMENT
OF DIGITAL SYSTEMS

1 Ιουνίου 2021

ΠΡΟΣΚΛΗΣΗ ΠΑΡΟΥΣΙΑΣΗΣ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Την Πέμπτη 2 Απριλίου και ώρα 13:00 π.μ. - 15:00 π.μ. θα πραγματοποιηθεί η παρουσίαση και αξιολόγηση της Διδακτορικής Διατριβής του κ. Αθανάσιου Γουδόση, Υποψηφίου Διδάκτορα της Σχολής Τεχνολογιών Πληροφορικής και Επικοινωνιών, του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστήμιου Πειραιώς. Η Διδακτορική Διατριβή φέρει τον τίτλο «**Εφαρμογές της Κρυπτογραφίας Βάσει Ταυτότητας στην Ηλεκτρονική Διακυβέρνηση και στη Ναυσιπλοΐα**». Στη διατριβή διερευνάται η πιθανή χρήση μηχανισμών Κρυπτογραφίας Βάσει Ταυτότητας (ΚΒΤ) αφενός στη ναυσιπλοΐα και ειδικότερα στην ασφάλεια του συστήματος Automatic Identification System (AIS), και αφετέρου στην ηλεκτρονική διακυβέρνηση και ειδικότερα στα συστήματα αναφοράς παραβατικών πράξεων. Η διατριβή εστιάζει στη διερεύνηση και πειραματική εφαρμογή προτάσεων βασισμένων σε σχήματα Κρυπτογραφίας Βάσει Ταυτότητας (ΚΒΤ) με απώτερο στόχο την επίλυση προβλημάτων Ηλεκτρονικής Διακυβέρνησης και την ασφάλεια της Ναυσιπλοΐας. Η ΚΒΤ είναι μία ιδιαίτερη μορφή κρυπτογράφησης δημόσιου κλειδιού, η οποία δεν χρησιμοποιεί πιστοποιητικά διότι το δημόσιο αναγνωριστικό κάθε οντότητας είναι το δημόσιο κλειδί της. Αυτή η μοναδική ιδιαιτερότητα της ΚΒΤ έχει προσελκύσει την προσοχή των ερευνητών, την τελευταία δεκαετία, στη διερεύνηση πιθανών εφαρμογών τις οποίες οι παραδοσιακές μεθοδολογίες κρυπτογράφησης δεν καλύπτουν επαρκώς. Η διατριβή προτείνει την εφαρμογή συγκεκριμένων υλοποιήσεων της ΚΒΤ στις έμπιστες διαδικτυακές επώνυμες και ανώνυμες αναφορές στον τομέα της Ηλεκτρονικής Διακυβέρνησης, καθώς και στην ενίσχυση της ασφάλειας της ναυσιπλοΐας στη Ναυτιλία. Στο πεδίο της ηλεκτρονικής διακυβέρνησης η διατριβή εξετάζει τη χρήση της ΚΒΤ, ιδιαίτερα των σχημάτων BLMQ-SKIBE και ECCSI-SAKKE , στην επίτευξη ανώνυμης επικοινωνίας σε βάθος χρόνου μεταξύ αναφερόντων και αρχών με το επιπλέον πλεονέκτημα της δυνατότητας της ανά πάσα στιγμή απόδειξης από τον ανώνυμο αναφέροντα της πραγματικής του ταυτότητας. Στη συνέχεια, αξιολογείται μία πειραματική υλοποίηση της πρότασης, βασισμένη στο σχήμα ECCSI-SAKKE, που απευθύνεται σε οργανισμούς με περιορισμένους πόρους (ανθρώπινους, οικονομικούς και υπολογιστικούς). Στο πεδίο της ναυσιπλοΐας, για την αντιμετώπιση των ζητημάτων ασφαλείας του AIS, προτείνεται η ανάπτυξη μιας υποδομής ΚΒΤ χωρίς πιστοποιητικά, σχεδιασμένης για τον

ΚΑΡΑΟΛΗ & ΔΗΜΗΤΡΙΟΥ 80 **TEL: 210.4142426-2373** **80, KARAOLI & DIMITRIOU STR.**
185 34 ΠΕΙΡΑΙΑΣ **FAX: 210.4142376** **185 34 P1RAEUS - GREECE**

ναυτιλιακό τομέα. Η πρόταση προσδίδει στο AIS δυνατότητες ταυτοποίησης και ελέγχου της ακεραιότητας των δεδομένων που εκπέμπονται, ψευδωνυμοποίηση του πομπού (ανωνυμία κατ' απαίτηση) και δυνατότητες κρυπτογράφησης.

Η εν λόγω παρουσίαση θα πραγματοποιηθεί μέσω της πλατφόρμας e-presence. Όσοι επιθυμούν να παρακολουθήσουν την παρουσίαση μπορούν να το δηλώσουν στην ηλεκτρονική διεύθυνση kpoupou@unipi.gr μέχρι την Παρασκευή, 25 Ιουνίου 2021.