ΟΜΙΛΙΑ

“Ασφάλεια Λογισμικού εκ Σχεδιασμού (Software Security-by-Design)”

Μιλτιάδης Σιάββας
Μεταδιδακτορικός Ερευνητής
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

ΠΕΡΙΛΗΨΗ – ABSTRACT

Η ομιλία αυτή θα παρουσιάσει την πρόσφατη ερευνητική δραστηριότητά μου στον χώρο της ασφάλειας πληροφοριακών συστημάτων, εστιάζοντας συγκεκριμένα στην ανάπτυξη ασφαλούς λογισμικού εκ σχεδιασμού. Θα παρουσιαστούν μηχανισμοί και τεχνικές που έχουν αναπτυχθεί στο πλαίσιο της ερευνητικής μου δραστηριότητας για την εξαγωγή, μοντελοποίηση και αξιολόγηση απαιτήσεων ασφάλειας, την αξιολόγηση της συμμόρφωσης λογισμικού ως προς κρίσιμες απαιτήσεις ασφάλειας, καθώς και την ανάλυση και αξιολόγηση της ασφάλειας κώδικα μέσω τεχνικών στατικής ανάλυσης και τεχνητής νοημοσύνης, με έμφαση στην αξιοποίηση Μεγάλων Γλωσσικών Μοντέλων (Large Language Models – LLMs). Παράλληλα, η ομιλία θα εστιάσει σε σύγχρονες ερευνητικές κατευθύνσεις που αφορούν τόσο την αξιοποίηση μηχανισμών τεχνητής νοημοσύνης για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων γενικότερα, όσο και την ασφάλεια, αξιοπιστία και ανθεκτικότητα μοντέλων και συστημάτων τεχνητής νοημοσύνης.

Short Bio: *Ο Δρ. Μιλτιάδης Σιάββας είναι Μεταδιδακτορικός Ερευνητής στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης (ΑΠΘ), όπου εργάζεται στο πλαίσιο του έργου EDF VICTORIOUS. Η μεταδιδακτορική του έρευνα εστιάζει στην αξιοποίηση προηγμένων τεχνικών τεχνητής νοημοσύνης για την ενίσχυση της ασφάλειας λογισμικού, πληροφοριακών συστημάτων και δικτύων. Παράλληλα, παρέχει υπηρεσίες εντεταλμένου διδάσκοντα τόσο στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών όσο και στο Τμήμα Πληροφορικής του ΑΠΘ. Προηγουμένως, εργάστηκε επί σειρά ετών ως Ερευνητικός Συνεργάτης στο Ινστιτούτο Πληροφορικής και Τηλεπικοινωνιών (ΙΠΤΗΛ) του Εθνικού Κέντρου Έρευνας και Τεχνολογικής Ανάπτυξης (ΕΚΕΤΑ), συμμετέχοντας σε πολυάριθμα ευρωπαϊκά ερευνητικά έργα Horizon, όπως τα SDK4ED, IoTAC, DOSS και ATHENA, αναλαμβάνοντας συχνά διαχειριστικούς ρόλους όπως τον ρόλο Τεχνικού Υπευθύνου και Επιστημονικού Υπευθύνου. Είναι κάτοχος διδακτορικού διπλώματος στην Ασφάλεια και Αξιοπιστία Λογισμικού από το Τμήμα Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών του Imperial College του Λονδίνου, υπό την επίβλεψη του καθηγητή Erol Gelenbe. Διαθέτει επίσης Δίπλωμα Μηχανικού από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης (ΑΠΘ), από το οποίο αποφοίτησε με άριστα. Τα ερευνητικά του ενδιαφέροντα εντάσσονται στο ευρύτερο πεδίο της ασφάλειας εκ σχεδιασμού (security-by-design) με ιδιαίτερη έμφαση στην ανάπτυξη ασφαλούς λογισμικού και*

πληροφοριακών συστημάτων αξιοποιώντας τόσο ντετερμινιστικές/συμβολικές τεχνικές όσο και τεχνικές τεχνητής νοημοσύνης. Τέλος, η πρόσφατη έρευνά του έχει επεκταθεί προς την ασφάλεια, την αξιοπιστία και την ανθεκτικότητα μοντέλων και συστημάτων τεχνητής νοημοσύνης. .

ΤΕΤΑΡΤΗ 17 ΙΟΥΝΙΟΥ 2026
12:20-13:20
ΑΙΘΟΥΣΑ ΣΕΜΙΝΑΡΙΩΝ