ΟΜΙΛΙΑ

" "Πόσο Ασφαλείς Είμαστε?": Η Επανάσταση στην Αρχιτεκτονική Συστημάτων και Επικοινωνιών μέσω Trusted Computing "

Αθανάσιος Γιαννέτσος
Adjunkt Associate Professor
Τεχνικό Πανεπιστήμιο Δανίας

ΠΕΡΙΛΗΨΗ – ABSTRACT

Στο σύγχρονο, ψηφιακά διασυνδεδεμένο περιβάλλον, οι παραδοσιακές μέθοδοι κυβερνοασφάλειας που βασίζονται αποκλειστικά στο λογισμικό (software) αποδεικνύονται συχνά ανεπαρκείς απέναντι σε εξελιγμένες και επίμονες απειλές (APTs). Αν και πρόσφατα έχουν προταθεί αρχιτεκτονικές ασφάλειας που υποστηρίζονται από το hardware, ένα τεράστιο ποσοστό ήδη ανεπτυγμένων, ενσωματωμένων συσκευών με περιορισμένους πόρους (resource-constrained devices) στερείται αυτών των δυνατοτήτων. Η πλειονότητα αυτών των συσκευών λειτουργεί σε επίπεδο "bare-metal", εκτελώντας κώδικα σε πλήρως προσβάσιμες και απροστάτευτες μνήμες, χωρίς λειτουργικό σύστημα ή βασικές εγγυήσεις ασφάλειας. Η ραγδαία εξέλιξη των δικτύων και η ανάγκη για απόλυτη ακεραιότητα των δεδομένων μάς αναγκάζουν να θέσουμε ένα κρίσιμο ερώτημα: *Πόσο ασφαλείς είμαστε πραγματικά όταν η ίδια η βάση των συστημάτων μας μπορεί να αμφισβητηθεί;* Η παρούσα εισήγηση εξετάζει τη ριζική μεταβολή του παραδείγματος (paradigm shift) στην ασφάλεια πληροφοριών μέσω του **Trusted Computing (Αξιόπιστη Υπολογιστική)**. Πρόκειται για μια αρχιτεκτονική επανάσταση που μεταφέρει τη ρίζα της εμπιστοσύνης (Root of Trust) από το ευάλωτο λογισμικό απευθείας στο υλικό (hardware), χρησιμοποιώντας τεχνολογίες όπως το TPM (Trusted Platform Module), και τα απομονωμένα περιβάλλοντα εκτέλεσης (Enclaves). Κατά την διάρκεια της παρουσίασης, θα αναλυθεί η δουλειά που έχουμε κάνει για τον σχεδιασμό τέτοιων trust anchors (HW-assisted attestation primitives) και πως μπορούν να βοηθήσουν στην ασφάλεια όλου του "device compute stack" αλλά και σε εφαρμογές κρίσιμης ασφάλειας. Θα παρουσιάσουμε τον οδικό χάρτη προς μια "ποσοτικοποίηση της εμπιστοσύνης" σε όλο το εύρος του Compute Continuum – μια πρόκληση που μπορεί να αντιμετωπιστεί μόνο με την εισαγωγή trust assessment μηχανισμών (σε επίπεδο HW και SW) για την μετατροπή όλων των συσκευών σε secure tokens, ως καταλυτικό παράγοντα για την ασφαλή επικοινωνία και την ανταλλαγή δεδομένων με άλλες οντότητες στο περιβάλλον τους.

Short Bio: Ο Θανάσης Γιαννέτσος έλαβε το διδακτορικό του δίπλωμα (Ph.D.) από το Πανεπιστήμιο του Άλμποργκ (Aalborg University) της Δανίας το 2012. Πριν αναλάβει τη θέση του Επικεφαλής της Ομάδας Ασφάλειας και Αξιόπιστης Υπολογιστικής (Head of Security and Trusted Computing Group) στην Ubitech Ltd, διετέλεσε Αναπληρωτής Καθηγητής στο Τμήμα Κυβερνοασφάλειας του Τεχνικού Πανεπιστημίου της Δανίας (DTU). Από το 2021 ο κ. Γιαννέτσος κατέχει την θέση Adjunkt Associate Professor στο DTU. Ο κ. Γιαννέτσος έχει επίσης εργαστεί ως Ανώτερος Ερευνητής (Senior Researcher) στην ομάδα Ασφάλειας Δικτυωμένων Συστημάτων του ΚΤΗ στη Σουηδία και, στη συνέχεια, ως Επίκουρος Καθηγητής στο Τμήμα Πληροφορικής του Πανεπιστημίου του Surrey (University of Surrey) στο Ηνωμένο Βασίλειο. Τα ερευνητικά του ενδιαφέροντα εκτείνονται από

τους μηχανισμούς ελέγχου πρόσβασης, penetration analysis και την προστασία από επιθέσεις (physical attacks), έως τα κρυπτογραφικά πρωτόκολλα και την εφαρμοσμένη κρυπτογραφία. Διαθέτει εξειδίκευση στις τεχνολογίες αξιόπιστης υπολογιστικής (trusted computing) και την ενσωμάτωσή τους για την επίτευξη προηγμένης πιστοποίησης (attestation), επιχειρησιακής διασφάλισης (operational assurance), καθώς και στον σχεδιασμό και την υλοποίηση ασφαλών πρωτοκόλλων που προστατεύουν την ιδιωτικότητα, και στη διαχείριση κινδύνων (risk management).

ΔΕΥΤΕΡΑ 15 ΙΟΥΝΙΟΥ 2026
12:20-13:20
ΑΙΘΟΥΣΑ ΣΕΜΙΝΑΡΙΩΝ