

## **Πτυχιακή/Διπλωματική Εργασία**

### **Ασφαλής Αποτύπωση της θέσης ενός κόμβου μέσα στο δίκτυο**

#### **(Trusted Location Reporting using TPM)**

Τα κινητά αδόμητα δίκτυα (Mobile Ad-Hoc networks) συνιστούν, όλο και πιο συχνά, βασικό εργαλείο για τον διαμοιρασμό δεδομένων μέσα σε αυτά. Αρχιτεκτονικά, αποτελούν ένα υβριδικό δίκτυο πλέγματος, με δυνατότητες επικοινωνίας μεταξύ των γειτονικών κόμβων. Λόγω όμως αυτής της πολύπλευρης επικοινωνίας, δημιουργούνται σοβαρά προβλήματα-δυσχέρειες στη διαχείριση των χρηστών και στη διασφάλιση της αυθεντικότητας. Η δυναμικά μεταβαλλόμενη τοπολογία ενός αδόμητου δικτύου, δημιουργεί την απαίτηση της ασφαλής εξακρίβωσης της θέσης του εκάστοτε κόμβου μέσα στο δίκτυο.

Μια σύγχρονη προσέγγιση για την υλοποίηση του παραπάνω αποτελεί η χρήση Trusted Platform Modules, ή αλλιώς TPM, ενός coprocessor που μπορεί να εκτελεί λειτουργίες όπως hash functions, asymmetric encryption και decryption, asymmetric signing και signature verification, symmetric encryption και decryption, symmetric signing (HMAC) και signature verification, και key generation.

Στόχος της παρούσας διπλωματικής εργασίας είναι η μελέτη-αξιολόγηση διαφόρων πρωτοκόλλων αποτύπωσης της θέσης, ο προγραμματισμός ενός TPM σύμφωνα με αυτά τα πρωτόκολλα με σκοπό τη δημιουργία ενός αξιόπιστου και ασφαλούς μηχανισμού και η εξαγωγή χρήσιμων συμπερασμάτων μέσω προσομοίωσης.

#### **Συνοπτικά οι στόχοι της εργασίας είναι (σε χρονική σειρά):**

1. Μελέτη και καταγραφή των διαφόρων πρωτοκόλλων αποτύπωσης της θέσης μέσα σε ένα αδόμητο δίκτυο
2. Μελέτη των δυνατοτήτων προγραμματισμού ενός TPM σε Java/C++
3. Αποκατάσταση επικοινωνίας ενός TPM με τα πρωτόκολλα αποτύπωσης της θέσης
4. Δημιουργία ενός ασφαλούς και αποδοτικού μηχανισμού αποτύπωσης της θέσης
5. Εξαγωγή συμπερασμάτων για το προτεινόμενο σχήμα μέσω πειραματικής αποτίμησης

#### **Τυπικά Χαρακτηριστικά Εργασίας**

**Χρόνος διεξαγωγής εργασίας:** 4 έως 6 μήνες

**Αριθμός Ατόμων:** 1-2

**Επιβλέπων Καθηγητής:** Αναπληρωτής Καθηγητής Ε. Χατζηευθυμιάδης e-mail: shadj@di.uoa.gr

**Συνεργάτες:** Ανέστης Παπακοτούλας, e-mail: aparakot@di.uoa.gr

**Προσ απαιτούμενα:** Προγραμματισμός σε Java/C++