ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Θέμα Διπλωματικής Εργασίας

Σχεδιασμός και ανάπτυξη ενός διακριτικού αυθεντικοποίησης (Android εφαρμογή) για ασφαλή πρόσβαση σε μια ιστοσελίδα

Design and development of an authentication token (Android application) for secure access to a website

Επιβλέπων: Δρ. Μηνάς Δασυγένης (mdasyg **(at)** ieee.org**) – http://arch.icte.uowm.gr**

Η αυθεντικοποίηση σε ένα πληροφοριακό σύστημα επιτυγχάνεται με έναν από τους τρεις παρακάτω τρόπους: (α) σε κάτι που γνωρίζει ο χρήστης, (π.χ. κωδικό), (β) σε κάτι που έχει ο χρήστης (π.χ. έξυπνη κάρτα τράπεζας) και (γ) σε μια σωματική ιδιαιτερότητα (πχ. αποτύπωμα παλάμης). Ο τυπικός και πιο δημοφιλής τρόπος αυθεντικοποίησης είναι ο πρώτος με τη χρήση του ονόματος χρήστη και κωδικού ασφαλείας. Υπάρχουν όμως, καταστάσεις που επιβάλουν την ταυτόχρονη υιοθέτηση πολλαπλών τρόπων πρόσβασης, όπως η χρήση του πρώτου και του δεύτερου τρόπου ελέγχου πρόσβασης. Το πιο αντιπροσωπευτικό παράδειγμα αυτών των καταστάσεων που απαιτεί επιπρόσθετες δικλείδες ασφαλείας, βρίσκεται στις ηλεκτρονικές συναλλαγές μέσω των περιβαλλόντων e-banking που παρέχουν οι τράπεζες. Συγκεκριμένα, ο χρήστης απαιτείται να εισάγει το όνομα χρήστη, τον κωδικό του και έναν αριθμό που δημιουργείται από μια android εφαρμογή παραγωγής μοναδικών αριθμών.

Οι πιο πρόσφατες εφαρμογές που παράγουν τους αριθμούς, έχουν υιοθετήσει ένα νέο πρότυπο του αλγόριθμου OTP (One-Time Password Algorithm), που βασίζεται στον αλγόριθμο HMAC SHA-1 (keyed-hash message authentication code) και ονομάζεται HMAC-based OTP (HOTP). Πρόκειται για έναν γεγονοδηγούμενο OTP αλγόριθμο, στον οποίο ένας μετρητής χρησιμοποιείται στον υπολογισμό του OTP και αυξάνεται, τόσο στον πελάτη (Android App), όσο και στον διακομιστή (website), μετά από κάθε χρήση. Αν είναι έγκυρος ο αριθμός για το συγκεκριμένο όνομα χρήστη, τότε εγκρίνεται η πρόσβαση, διαφορετικά απορρίπτεται.

Σε αυτή τη διπλωματική εργασία πρόκειται να αναπτυχθεί ένα σύστημα λογισμικού που θα επιδεικνύει την συγκεκριμένη λειτουργία. Συγκεκριμένα, αφού γίνει η βιβλιογραφική έρευνα για τον αλγόριθμο που θα χρησιμοποιηθεί για την αυθεντικοποίηση, θα ξεκινήσει η ανάπτυξη μια android εφαρμογής, που θα χρησιμοποιεί τον αλγόριθμο αυτό για να παράγει προσωπικούς αριθμούς αυθεντικοποίησης για έναν χρήστη. Ταυτόχρονα, θα αναπτυχθεί σε PHP/mysql, μια ιστοσελίδα που θα επιβεβαιώνει τους αριθμούς αυτούς για το συγκεκριμένο όνομα χρήστη.

Απαιτήσεις: Προγραμματισμός Διαδικτύου, Κινητή Υπολογιστική, Ανάλυση και Σχεδίαση Αλγορίθμων

Πλεονεκτήματα: Ο φοιτητής που θα φέρει εις πέρας αυτή την εργασία θα αποκτήσει μια καλή γνώση του σχεδιασμού πληροφοριακών συστημάτων, του προγραμματισμού σε κινητά τηλέφωνα και των προβλημάτων που προκύπτουν σε πραγματικά έργα. Η ενασχόλησή του με αυτό το θέμα θα του δώσει τα κατάλληλα εφόδια για να ασχοληθεί με το σχεδιασμό σύνθετων android εφαρμογών που συνδέονται, είτε με τις ηλεκτρονικές συναλλαγές (e-banking), είτε με οτιδήποτε άλλο.