ΠΑΝΕΠΙΣΤΗΜΙΟ
ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ
ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Θέμα Διπλωματικής Εργασίας

Σχεδιασμός και υλοποίηση συσκευής αυθεντικοποίησης με τη VHDL

Design and Implementation of VHDL authentication device

Επιβλέπων: Δρ. Μηνάς Δασυγένης (mdasyg@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 (π.χ. 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 προσωπική συσκευή παραγωγής μοναδικών αριθμών.

Οι συσκευές που παράγουν τους αριθμούς, εκτελούν έναν αλγόριθμο που βασίζεται στο RSA, ο οποίος δέχεται ως είσοδο το σειριακό αριθμό της συσκευής και την τρέχουσα ώρα. Ο αριθμός που παράγεται ισχύει για λίγα λεπτά. Το πληροφοριακό σύστημα στο διακομιστή είτε εκτελεί τον ίδιο αλγόριθμο με είσοδο την τρέχουσα ώρα και το σειριακό αριθμό της συσκευής (ο οποίος είναι αποθηκευμένος στη βάση δεδομένων και συνδέεται με το όνομα χρήστη), είτε χρησιμοποιεί έναν πιο απλό αλγόριθμο επιβεβαίωσης του μοναδικού αριθμού που εισήγαγε ο χρήστης. 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 και υλικού που θα επιδεικνύει τη συγκεκριμένη λειτουργία. Συγκεκριμένα, αφού γίνει η βιβλιογραφική έρευνα για τους αλγορίθμους που χρησιμοποιούνται για αυθεντικοποίηση βασισμένη σε συσκευή, θα γίνει η υλοποίηση ενός αλγορίθμου σε γλώσσα περιγραφής υλικού VHDL, που θα παράγει προσωπικούς αριθμούς αυθεντικοποίησης για ένα χρήστη. Ο αλγόριθμος θα απεικονιστεί σε πραγματικές αναπτυξιακές πλακέτες FPGA που υπάρχουν στο εργαστήριο ενώ ο αριθμός θα εμφανίζεται στο LCD της πλακέτας. Ταυτόχρονα, θα αναπτυχθεί σε PHP/mysql ο αλγόριθμος επιβεβαίωσης των αριθμών αυτών για το συγκεκριμένο όνομα χρήστη.

Απαιτήσεις: Προγραμματισμός Διαδικτύου, Αρχιτεκτονική Υπολογιστών, Ενσωματωμένα συστήματα, VHDL

Πλεονεκτήματα: Ο φοιτητής που θα φέρει εις πέρας αυτή την εργασία θα αποκτήσει μια καλή γνώση του σχεδιασμού πληροφοριακών συστημάτων, του προγραμματισμού, της διεπαφής hardware-software 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 ενσωματωμένων συστημάτων που συνδέονται με τις ηλεκτρονικές συναλλαγές (e-banking).