Ελεγχόμενη πρόσβαση σε κλειστό χώρο με χρήση ηλεκτρονικού υπολογιστή

Γιώργος Σταματελάτος και Γιώργος Δροσάτος
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Δημοκρίτειο Πανεπιστήμιο Θράκης
Email: {georstam2,gdrosato}@ee.duth.gr

***Περίληψη*—Στα πλαίσια αυτής της δουλειάς υλοποιήσαμε μία πλατφόρμα για το άνοιγμα μιας πόρτας χρησιμοποιώντας σύγχρονες τεχνολογίες, όπως αναγνώριση δακτυλικού αποτυπώματος [1] και δικτυακής διαχείρισης. Εξηγούμε τον τρόπο με τον οποίο το πετύχαμε καθώς και τα εργαλεία που χρησιμοποιήσαμε τόσο σε επίπεδο υλικού όσο και λογισμικού.**

I. Εισαγωγη

Ο συμβατικός τρόπος ανοίγματος μιας πόρτας με χρήση κλειδιού παρουσιάζει μειονεκτήματα τόσο στον τομέα της ασφάλειας όσο και της ευχρηστίας, πρόβλημα το οποίο γίνεται εντονότερο σε χώρους που απαιτείται η πρόσβαση από πολλαπλά άτομα (π.χ. χώρος εργαστηρίου). Στη δική μας περίπτωση η ενίσχυση της ασφάλειας επιτυγχάνεται με χρήση κωδικού πρόσβασης ή βιομετρικών χαρακτηριστικών (π.χ. δακτυλικό αποτύπωμα), τεχνικές που είναι λιγότερο ευπαθείς σε παραβιάσεις. Επιπλέον, η χρήση τέτοιων τεχνικών θεωρείται πιο εύχρηστη διότι: (i) αποδεσμεύει το χρήστη από την κατοχή κλειδιού, (ii) επιτρέπει την εύκολη διαχείριση των ατόμων που έχουν πρόσβαση, χωρίς να απαιτείται αλλαγή κλειδαριάς, και (iii) προσφέρει πρόσθετη δυνατότητα επιβολής χρονικής διάρκειας πρόσβασης του εκάστοτε ατόμου.

Στην υλοποίησή μας κάνουμε χρήση ηλεκτρονικού υπολογιστή ενώ η ταυτοποίηση των ατόμων επιτυγχάνεται με τη χρήση συνθηματικού (μέσω πληκτρολογίου ή διαδικτυακά) καθώς επίσης και μέσω δακτυλικού ίχνους (fingerprint). Στην εργασία αυτή, και για τις δύο μεθόδους που αναφέρθηκαν, εξετάζουμε το υλικό που χρειάζεται για μια τέτοια εγκατάσταση και περιγράφουμε τον τρόπο λειτουργίας του λογισμικού που καθιστά εφικτό το εγχείρημα. Τέλος, αναφέρουμε τα συμπεράσματά μας καθώς επίσης και τρόπους βελτίωσης της πλατφόρμας ή πιθανές επεκτάσεις στη χρήση της.

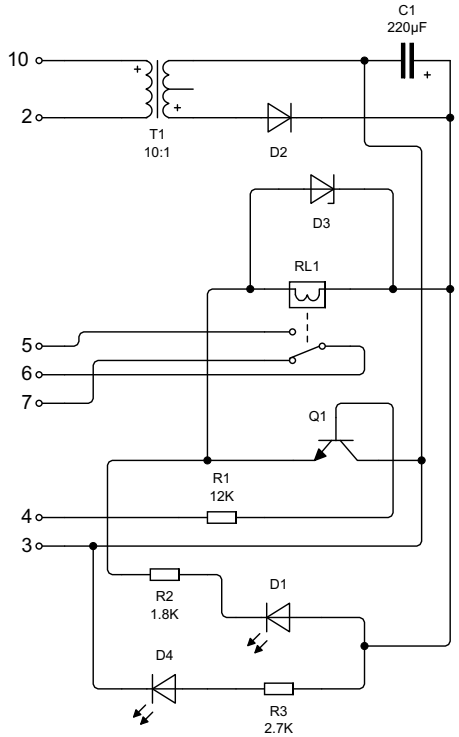
II. Υλικο

Ο απαραίτητος εξοπλισμός αποτελείται από έναν ηλεκτρονικό υπολογιστή, ένα τυπωμένο κύκλωμα και τέλος μια ηλεκτρική κλειδαριά.

Υπολογιστής. Το κύριο στοιχείο στο οποίο βασίζεται η πλατφόρμα μας είναι ένας ηλεκτρονικός υπολογιστής χαμηλών επιδόσεων και μικρών διαστάσεων (όπως Η/Υ προτύπου pico-itx [2]) με λειτουργικό σύστημα Linux (Ubuntu Server 9.04). Ο παραπάνω υπολογιστής διαθέτει παράλληλη θύρα για επικοινωνία με το τυπωμένο κύκλωμα που ελέγχει την ηλεκτρική κλειδαριά, πληκτρολόγιο και συσκευή ανάγνωσης δακτυλικού αποτυπώματος.

Για τη λειτουργία του συστήματός μας ο Η/Υ είναι αυτός που εχει το μεγαλύτερο φόρτο εργασίας. Κατάλληλο λογισμικό που εκτελείται στον υπολογιστή, αναλαμβάνει τον έλεγχο ταυτοποίησης (αν το συνθηματικό ή το fingerprint είναι έγκυρο) και κατόπιν, αν ο έλεγχος είναι επιτυχής, εφαρμόζεται τάση σε έναν από τους ακροδέκτες της παράλληλης θύρας για ένα σύντομο χρονικό διάστημα (5 δευτερόλεπτα). Το τυπωμένο κύκλωμα που είναι συνδεδεμένο στην παράλληλη θύρα ενεργοποιεί ή όχι το κύκλωμα της ηλεκτρικής κλειδαριάς.

Τυπωμένο κύκλωμα. Ένα εσωτερικά τροφοδοτούμενο τυπωμένο κύκλωμα που φαίνεται στο Σχήμα 1 περιέχει τα κατάλληλα ηλεκτρονικά μέρη για τη μετατροπή της πληροφορίας που μεταφέρεται από τον υπολογιστή σε ισχύ ικανή να ξεκλειδώσει την κλειδαριά. Το κύριος μέρος του είναι ένα τρανζίστορ που με την εφαρμογή τάσης ενεργοποιεί έναν ηλεκτρονόμο, ο οποίος είναι τοποθετημένος σε σειρά με ένα μετασχηματιστή 12V AC και την ηλεκτρική κλειδαριά.



Σχήμα 1. Κύκλωμα ελέγχου ηλεκτρικής κλειδαριάς. 10-2: Τάση τροφοδοσίας 230V AC, 5-6: Έλεγχος κλειδαριάς, 4-3: Παράλληλη θύρα.

III. Λογισμικο

Το λογισμικό που εκτελείται στον ηλεκτρονικό υπολογιστή αναπτύχθηκε στις γλώσσες C, C++ και C#/MONO και είναι οργανωμένο σε διακριτά μέρη, τα οποία περιγράφονται πιο κάτω.

Υπηρεσία ταυτοποίησης. Η πλατφόρμα του λογισμικού βασίζεται σε μια υπηρεσία (daemon) γραμμένη σε C# και περιβάλλον MONO που είναι υπεύθυνη για το μεγαλύτερο ποσοστό της διαδικασίας ταυτοποίησης που αναφέρθηκε. Αξίζει να σημειωθεί ότι στην ουσία η υπηρεσία ταυτοποίησης είναι μια δικτυακή υπηρεσία (TCP Server). Εξασφαλίζεται έτσι ο διαχωρισμός μεταξύ της εισόδου και της επεξεργασίας επιτυγχάνοντας μεγαλύτερη ευελιξία για το σύστημα. Ένα μήνυμα που αποστέλλεται στην υπηρεσία περιέχει τα ακόλουθα πεδία:

- *Σκοπός της αποστολής*. Εκτός από ένα αίτημα ανοίγματος της πόρτας, υπάρχουν και δυνατότητες όπως εισαγωγή έγκυρου συνθηματικού ή αλλαγή κωδικού χρήστη.
- *Δεδομένα της αποστολής*. Στην περίπτωση του αιτήματος ανοίγματος της πόρτας, τα δεδομένα είναι το συνθηματικό ή η εικόνα του fingerprint ενώ στην περίπτωση προσθήκης συνθηματικού τα δεδομένα αποτελούνται από το προς εισαγωγή συνθηματικό καθώς επίσης και από ένα έγκυρο υπάρχον συνθηματικό. Με αυτόν τον τρόπο πιστοποιείται ότι το δικαίωμα πρόσβασης στο χώρο από το *νέο* χρήστη έχει δοθεί από άτομο που έχει ήδη πρόσβαση.

Ως παράδειγμα θα αναφέρουμε τη συμβολοσειρά: "door open pass 1234". Η ακολουθία αυτή, κωδικοποιημένη σε UTF-16 [3] (και συγκεκριμένα little endian), ζητάει από την υπηρεσία να ανοίξει την πόρτα χρησιμοποιώντας ως συνθηματικό το αλφαριθμητικό "1234". Η υπηρεσία (αν το συνθηματικό είναι έγκυρο) θα εφαρμόσει τάση σε έναν από τους ακροδέκτες της παράλληλης, με τη βοήθεια της βιβλιοθήκης parapin [4]. Σημειώνεται ότι το αίτημα ανοίγματος με χρήση δακτυλικού αποτυπώματος επιτυγχάνεται με μια ακολουθία της μορφής "door open print" ακολουθούμενο με τη δεκαεξαδική αναπαράσταση της εικόνας που έχει διαβάσει ο αναγνώστης. Η υπηρεσία χρησιμοποιεί τη βιβλιοθήκη ανοιχτού κώδικα fprint [5] για την επαλήθευση των δακτυλικών αποτυπωμάτων.

Τα ευαίσθητα προσωπικά δεδομένα (δακτυλικά αποτυπώματα) των χρηστών αποθηκεύονται κρυπτογραφημένα και οι κωδικοί πρόσβασης αποθηκεύονται σε μορφή SHA-1 [6]. Η δικτυακή επικοινωνία με τον daemon όμως δε χρησιμοποιεί SSL socket και κατ' επέκταση δεν είναι ασφαλής για επικοινωνία μέσω δικτύου, είτε τοπικού είτε του Διαδικτύου. Αυτό όμως δεν αποτελεί σημαντικό πρόβλημα μιας και οι τέσσερις εφαρμογές εισόδου της υπηρεσίας εκτελούνται τοπικά.

Εφαρμογές εισόδου. Η υπηρεσία ταυτοποίησης δέχεται σαν είσοδο απλές συμβολοσειρές. Για να προκύψουν, όμως, αυτές χρειάζονται επιπλέον εφαρμογές που θα μετατρέπουν τη φυσική είσοδο (κωδικός, φωτογραφία αποτυπώματος) σε μια ακολουθία επεξεργάσιμη από την υπηρεσία ταυτοποίησης. Οι εφαρμογές αυτές εκτελούνται παράλληλα και συνεχώς.

- *Αναγνώστης πληκτρολογίου*. Διαβάζει συνεχώς συμβολοσειρές που πληκτρολογούνται και αποστέλλει πακέτα τύπου "door open pass".
- *Αναγνώστης δακτυλικού αποτυπώματος*. Λειτουργεί παρόμοια με τον αναγνώστη πληκτρολογίου και χρησιμοποιεί πακέτα τύπου "door open print".
- *Δικτυακή διεπαφή*. Η εγκατάστασή μας φιλοξενείται δικτυακά στον ιστότοπο https://portoula.dyndns.org/ όπου έχουν υλοποιηθεί όλα τα απαραίτητα χαρακτηριστικά του daemon για τη λειτουργία του συστήματος. Πετυχαίνεται έτσι το άνοιγμα της πόρτας χωρίς να υπάρχει φυσική επαφή του ατόμου που ταυτοποιείται. Η ιστοσελίδα λειτουργεί με ασφαλή σύνδεση που χαρακτηρίζεται από το πρόθεμα HTTPS έτσι ώστε να μη μεταφερθεί ως plaintext μέσω Διαδικτύου το συνθηματικό.
- *Εφαρμογή Android*. Με βάση την παραπάνω διεπαφή αναπτύχθηκε εφαρμογή για το λειτουργικό σύστημα Android που με χρήση αιτημάτων POST πετυχαίνει το άνοιγμα της πόρτας. Αξίζει να σημειωθεί ότι η αποστολή από τη συσκευή δε γίνεται απευθείας με τη μορφή αιτήματος TCP για να αποφευχθεί η αποστολή του συνθηματικού. Αντ' αυτού αποστέλλεται κρυπτογραφημένο στη δικτυακή διεπαφή η οποία με τη σειρά της επικοινωνεί τοπικά με την υπηρεσία ταυτοποίησης.

IV. Συμπερασματα

Με την εργασία αυτή καταφέραμε να ελέγξουμε το άνοιγμα μιας πόρτας με ταυτοποίηση προσώπου, η οποία επιτυγχάνεται είτε με τη γνώση ενός συνθηματικού είτε μέσω του δακτυλικού αποτυπώματος. Η επίτευξη των παραπάνω έγινε χρησιμοποιώντας ένα ευρύ φάσμα τεχνολογιών από το αντικείμενο του Ηλεκτρολόγου Μηχανικού, όπως έννοιες ηλεκτρικών στοιχείων, ηλεκτρονικής σχεδίασης, ψηφιακών συστημάτων, λογισμικού, επεξεργασία βιομετρικών χαρακτηριστικών κ.ά.

Αρκετά σημεία στην πλατφόρμα μπορούν να επεκταθούν τόσο σε επίπεδο υλικού όσο και λογισμικού. Εξετάζεται το ενδεχόμενο να εισαχθεί η αναγνώριση προσώπου (face recognition) ως εναλλακτική μέθοδος ταυτοποίησης, η οποία μπορεί να αποδειχθεί πιο ασφαλής αλλά και πιο εύχρηστη. Στο θέμα του ηλεκτρονικού υπολογιστή έχουμε προσαρμόσει το λογισμικό για υποστήριξη επικοινωνίας μέσω USB, που είναι πιο δημοφιλές πρωτόκολλο, ενώ μελλοντικά θα μπορούσε να χρησιμοποιηθεί ένας ακόμα μικρότερος υπολογιστής, όπως ο raspberry pi [7]. Τέλος, το σύστημα αυτό θα μπορούσε να γίνει μέρος μιας εγκατάστασης έξυπνου σπιτιού.

Αναφορες

[1] Maltoni D., Maio D., Jain A.K. and Prabhakar S. Handbook of fingerprint recognition. Springer-Verlag New York Inc, 2009.
[2] Wikipedia. PICO_ITX, Μάρτιος 2012. http://en.wikipedia.org/wiki/Pico_ITX.
[3] Wikipedia. UTF-16, Μάρτιος 2012. http://en.wikipedia.org/wiki/UTF-16.
[4] ELSON Jeremy. Parapin: a Parallel Port Pin Programming Library for Linux. Marina del Rey: University of Southern California, 2000. http://www.circlemud.org/pub/jelson.
[5] Freedesktop.org. The fprint project, Μάρτιος 2012. http://www.freedesktop.org/wiki/Software/fprint.
[6] Wikipedia. SHA-1, Μάρτιος 2012. http://en.wikipedia.org/wiki/SHA-1.
[7] The Raspberry Pi Foundation. Raspberry Pi: An ARM GNU/Linux box for $25, Μάρτιος 2012. http://www.raspberrypi.org/.