

Κατασκευή Έξυπνης, Τηλεχειριζόμενης
Κλειδαριάς Θυροτηλεφώνου με χρήση
Τεχνολογιών Αιχμής

Πανεπιστήμιο Πειραιώς

Κυριάκος Δ. Γιαννάκης

Day Test Year

Abstract

TODO

Contents

1 Εισαγωγή	2
1.1 Internet of Things	2
1.2 Αυτοματισμοί Σπιτιού - Home Automation	2
1.3 Σκοπός του PiLock	3
2 Δομή του PiLock	4
2.1 Σύντομη Περιγραφή Λογισμικού Εξυπηρετητή - PiLock Server	4
2.2 Σύντομη Περιγραφή Λογισμικού Πελάτη - PiLock Client	4
2.3 Υλικό - Hardware	5
2.3.1 Raspberry Pi Zero W	5
2.3.2 Relay Module	6
2.3.3 Arduino UNO	6
2.3.4 Λοιπό Hardware	7
3 Συστήματα Ελέγχου Πρόσβασης Πολυκατοικιών/Σπιτιών	9
4 Νέος μηχανισμός ξεκλειδώματος	11
4.1 Προετοιμασία του Raspberry Pi	11
4.1.1 Άλλαγή των προεπιλεγμένων στοιχείων πρόσβασης	12
4.1.2 Ενημέρωση του Raspbian	12
4.1.3 Ανάθεση στατικής διεύθυνσης IP	12
4.2 Σύνδεση με το Relay	13
4.2.1 Σύνδεση χωρίς την χρήση Arduino	13
4.2.2 Σύνδεση με την χρήση Arduino	13
5 Προγραμματιστικό Περιβάλλον - Τεχνολογίες που χρησιμοποιήθηκαν	16
5.1 Η σημασία χρήσης δωρεάν λογισμικού ανοικτού κώδικα κατά την ανάπτυξη του PiLock	16
5.2 Version Control	17

Chapter 1

Εισαγωγή

Στον σημερινό κόσμο, οι τεχνολογικές μιας ανάγκες γίνονται ολοένα και πιο πολύπλοκες. Κάθε μέρα βγαίνουν στην επιφάνεια νέες τεχνολογικές διευκολύνσεις για τον άνθρωπο, σκοπός των οποίων είναι να κάνουν την διαβίωσή του πιο "έξυπνη", δίνοντάς του τον μέγιστο έλεγχο σε κάθε σημείο της ζωής του. Με την άνθιση του internet of things, γίνεται εύκολη η διασύνδεση πολλών συσκευών (από την μικρότερη ως την μεγαλύτερη), με σκοπό τον έλεγχό τους απομιαχρυσμένα.

Σκοπός της παρούσας πτυχιακής εργασίας είναι να περιγράψει την πλήρη διαδικασία του σχεδιασμού και υλοποίησης ενός συστήματος ελέγχου αλειδαριάς σπιτιού/γραφείου, γνωστό ως PiLock.

Η εφαρμογή υλοποιήθηκε, στο μεγαλύτερο μέρος της, χρησιμοποιώντας λογισμικό τελευταίας τεχνολογίας, πράγμα που μιας εγγυάται την μέγιστη ευελιξία όσων αφορά την ανάπτυξη, πράγμα που ισοδυναμεί με μέγιστη ταχύτητα ανάπτυξης και αυξημένη ασφάλεια.

1.1 Internet of Things

Ο όρος "Internet of Things" (IoT) χρησιμοποιήθηκε πρώτη φορά από τον Kevin Ashton το 1999 σε μία παρουσίασή του στην Procter & Gamble (P&G) [1]. Ο όρος επινοήθηκε προκειμένου να μπορεί να τονιστεί η δύναμη της (τότε) δημοφιλούς ιδέας της χρήσης της τεχνολογίας RFID σε συστήματα εφοδιαστικών αλυσίδων εταιριών για παρακολούθηση εμπορευμάτων. Πλέον, ο όρος Internet of Things χρησιμοποιείται προκειμένου να χαρακτηριστούν συσκευές (μικρές ή μεγάλες) με δυνατότητα σύνδεσης στο Internet. Κάποια παραδείγματα είναι τα αυτοκίνητα με ενσωματωμένους αισθητήρες, τα έξυπνα σπίτια (τα οποία αποτελούνται από μια πληθώρα έξυπνων συσκευών), καθώς επίσης και συγκεχριμένες συσκευές παρακολούθησης υγείας (όπως πχ. συσκευές παρακολούθησης καρδιακού ρυθμού) με δυνατότητα σύνδεσης στο διαδίκτυο.

Οι δυνατότητες που έχουν οι συγκεχριμένες συσκευές τις καθιστούν ικανές για σύνδεση στο internet, και κατ'επέκταση, αυξάνουν σημαντικά τις λειτουργίες τους, προσδίδοντας μεγαλύτερο έλεγχο στον χρήστη.

1.2 Αυτοματισμοί Σπιτιού - Home Automation

Μία από τις πιο σημαντικές υποκατηγορίες των συσκευών Internet of Things είναι οι συσκευές αυτοματισμού σπιτιών (Home Automation Devices, Domotics

[2]). Οι συσκευές αυτές δίνουν στον χρήστη τους την δυνατότητα να διαχειριστεί διάφορες συσκευές του σπιτιού/γραφείου του. Οι συσκευές αυτές μπορεί να είναι συσκευές κλιματισμού, φωτισμός, συστήματα διασκέδασης (Home Theaters, Music Stereos, κτλ...), καθώς επίσης και συστήματα συναγερμού ή και διαχείρησης πρόσβασης. To PiLock ανήκει στην τελευταία αυτή κατηγορία.

Συνήθως, οι συσκευές αυτές συνδέονται σε ένα κεντρικό κόμβο (Hub) προκειμένου να ελέγχονται όλες από ένα μοναδικό σημείο. Η δυνατότητα αυτή μπορεί να προστεθεί σε μία επόμενη έκδοση του PiLock (βλ. μελλοντικά σχέδια). Την παρούσα χρονική στιγμή, δεν υπάρχει αυτή η δυνατότητα.

1.3 Σκοπός του PiLock

Το PiLock ανήκει στην κατηγορία συσκευών ”έξυπνου σπιτιού” (Smart Home). Σκοπός του είναι να παρέχει στον χρήστη την δυνατότητα να ξεκλειδώνει εύκολα την εξώπορτα/πόρτα του σπιτιού/γραφείου του, μέσω του SmartPhone ή του SmartWatch του, όλα αυτά χρησιμοποιώντας το ασφαλέστερο δυνατόν περιβάλλον, προκειμένου να αποφευχθεί εισβολή τρίτων.

Μέσω του **PiLock Administration Control Panel (PiLock AdminCP)**, δίνουμε στον διαχειριστή του συστήματος ένα εύχρηστο περιβάλλον διαχείρησης από το οποίο μπορεί εύκολα και γρήγορα να διαχειρίζεται το PiLock. Δίνεται δυνατότητα διαχείρησης των **εξουσιοδοτημένων χρηστών** (χρήστες που μπορούν να ξεκλειδώσουν την πόρτα μέσω του PiLock), δυνατότητα λήψης ζωτικής σημασίας πληροφοριών για το σύστημα, καθώς επίσης και της δυνατότητας ξεκλειδώματος της πόρτας απευθείας μέσω του πίνακα διαχείρησης, χωρίς να χρειάζεται να γίνει χρήση εφαρμογής (AdminCP Unlock).

Ένας από τους στόχους, κατά τον σχεδιασμό του PiLock ήταν η διατήρηση του κόστους στο χαμηλότερο δυνατόν. Για να επιτευχθεί ο στόχος αυτός, χρησιμοποιήθηκε αυστηρά δωρεάν λογισμικό ανοικτού κώδικα, καθώς επίσης και εξαρτήματα εύκολα προσκομίσιμα (βλ. Κεφάλαιο 2, Δομή του PiLock).

Chapter 2

Δομή του PiLock

To PiLock αποτελείται από 2 κύρια μέρη: Τον εξυπηρετητή (Server) και τον πελάτη (Client).

2.1 Σύντομη Περιγραφή Λογισμικού Εξυπηρετητή - PiLock Server

Ο εξυπηρετητής αποτελείται από το Hardware που χρειάζεται προκειμένου να λειτουργήσει το PiLock, καθώς επίσης και το αντίστοιχο λογισμικό υπεύθυνο για την διαχείρηση της κλειδαριάς, από όλες τις απόψεις. Πιο συγκεκριμένα, το λογισμικό είναι υπεύθυνο για:

- Την διαχείριση του Hardware υπεύθυνου για την λειτουργία του μηχανισμού ξεκλειδώματος.
- Την αυθεντικοποίηση των ήδη υπάρχοντων χρηστών.
- Την δημιουργία νέων χρηστών, ικανών για αυθεντικοποίηση (εξουσιοδοτημένοι χρήστες).
- Την τήρηση ιστορικού αυθεντικοποιήσεων (επιτυχών ή μή).

Το λογισμικό του εξυπηρετητή αναλύεται πλήρως στην αντίστοιχη ενότητα.

2.2 Σύντομη Περιγραφή Λογισμικού Πελάτη - PiLock Client

Η πλευρά του πελάτη αποτελείται από την εφαρμογή του PiLock, σχεδιασμένη για κινητά που τρέχουν Android, καθώς επίσης και από την εφαρμογή σχεδιασμένη για Android Wear Smartwatches.

Πιο συγκεκριμένα, οι εφαρμογές στο πεδίο του πελάτη είναι υπεύθυνες για:

- Σύνδεση στην πλατφόρμα του PiLock*.
- Αποστολή αιτημάτων ξεκλειδώματος.
- Αποστολή αιτημάτων αλλαγής PIN*.

Οι δυνατότητες που είναι σημειωμένες με τον αστερίσκο (*) είναι διαθέσιμες αποκλειστικά στην εφαρμογή για κινητά (mobile app) και όχι στην εφαρμογή για Android Wear.

2.3 Υλικό - Hardware

Όπως αναφέραμε και στην εισαγωγή, ένας εκ των στόχων από τις πρώτες μέρες του σχεδιασμού του PiLock ήταν να υλοποιηθεί το Project με όσο το δυνατόν λιγότερο κόστος. Προκειμένου αυτό να είναι εφικτό, χρησιμοποιήσαμε υλικό εύκολα προσκομίσιμο και, όπου ήταν δυνατόν, Open Source Hardware.

2.3.1 Raspberry Pi Zero W

”Εγκέφαλος” όλης της κατασκευής είναι το Raspberry Pi Zero W (RPi Zero W), ένας υπολογιστής μοναδικής πλακέτας (Single Board). Σχεδιάζεται από το Raspberry Pi Foundation στην Αγγλία και η χυκλοφορία του ξεκίνησε τον Φεβρουάριο του 2017. Σκοπός του RPi Zero W είναι να συμπληρώσει το προηγούμενο μοντέλο, το Raspberry Pi Zero, φέρνοντας δυνατότητες συνδεσιμότητας WiFi 802.11n και BlueTooth 4.0 χωρίς Hardware κάποιου τρίτου (μέχρι προτίστως έπρεπε να χρησιμοποιηθεί κάποιο WiFi ή BlueTooth Dongle προκειμένου να υπάρξει αυτή η συνδεσιμότητα) [3].



Εικόνα 2.1: Το Raspberry Pi Zero W.

Στην ”καρδιά” του RPi Zero W υπάρχει ένας Broadcom BCM2835, 32-bit επεξεργαστής αρχιτεκτονικής ARMv6, χρονισμένος στο 1Ghz. Για μινήμη τυχαίας προσπέλασης χρησιμοποιούνται 512MB Low Power Double Data Rate 2 (LPDDR2) RAM. Πανω στο RPi Zero W δεν υπάρχει αποθηκευτικός χώρος, οπότε χρησιμοποιείται μια κάρτα MicroSD.

Ένα από τα σημαντικότερα σημεία ενός RPi Zero W είναι οι **δέκτες Εισόδου/Εξόδου Γενικού Σκοπού (GPIO)**. Μέσω αυτών καθίσταται δυνατόν να συνδεθεί το RPi με μια πληθώρα εξωτερικών αισθητήρων, διακοπών (Relay Modules), πλακετών επέκτασης (γνωστά ως HATs), και εξαρτημάτων και να αντλήσει πληροφορίες ή να τα ελέγξει.

2.3.2 Relay Module

Προκειμένου να μπορέσει να συνδεθεί το RPi με το ήδη υπάρχον σύστημα ξεκλειδώματος, χρειάζεται ένας ηλεκτρονικά ελεγγχόμενος διακόπτης. Θα χρησιμοποιηθεί ένα Relay Module. Τα Relay Modules χρησιμοποιούνται ως διακόπτες προκειμένου να ελέγχονται κυκλώματα μέσω υπολογιστών/μικροελεγκτών, οι οποίοι λειτουργούν μέσω σημάτων μικρής ισχύος^[5].

Τα Relay Modules κυκλοφορούν σε πολλούς τύπους. Οι τρείς κυριότεροι είναι:

- 5V Compatible, Active Low.
- 5V/3.3V Compatible, Active High.
- 3.3V Compatible Active High/Low.

Το Raspberry Pi, εφόσον λειτουργεί σε λογική 3.3V, είναι συμβατό με τους 2 τελευτέους τύπους. Αν θελήσουμε να χρησιμοποιήσουμε ένα Relay Module που να λειτουργεί σε λογική 5V και είναι Active Low, θα χρειαστεί να χρησιμοποιήσουμε ένα Arduino.

Τα Relay Modules αποτελούνται από ένα Relay τύπου SRD, έναν φωτοσυζευκτή (Optocoupler), ευθύνη του οποίου είναι να απομονώνει το κύκλωμα ώστε να μην επηρεάσει η υψηλή τάση (σε περίπτωση που χρησιμοποιείται από το σύστημα ξεκλειδώματος του κτηρίου) το υπόλοιπο κύκλωμα, ένα Transistor και μια δίοδο.

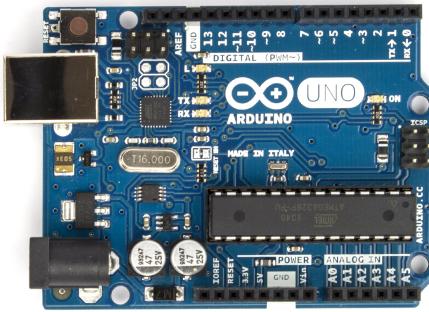
2.3.3 Arduino UNO

Το Arduino UNO είναι ένας Ανοικτού-Κώδικα (Open Source) μικροελεγκτής σχεδιασμένος από την Arduino.cc. Είναι βασισμένος πάνω στον ATmega328 microcontroller της Atmel. Μπορεί να χρησιμοποιηθεί προκειμένου να χειρίζεται και να αντλεί πληροφορίες από διάφορα εξαρτήματα στον φυσικό κόσμο. Εξαιτίας της μεγάλης ευελιξίας του έχει γίνει μία από τις δημοφιλέστερες επιλογές για κατασκευαστές, οι οποίοι το χρησιμοποιούν για μια τεράστια γκάμια εφαρμογών^[6].

Το Arduino UNO μπορεί να χρησιμοποιηθεί σε περίπτωση που δεν χρησιμοποιηθεί κάποιο Relay συμβατό με το Raspberry Pi (βλ. 2.3.2 Relay Module), αφού να λειτουργεί με λογική 5V.

Μπορεί, έναντι του Arduino UNO, και προκειμένου να εξοικονομήσει χώρος, να χρησιμοποιηθεί ένα Arduino Nano, το οποίο έχει όλες τις αναγκαίες λειτουργίες για την λειτουργία του PiLock.

Ρεύμα για την λειτουργία του Arduino παρέχεται από την θύρα Micro USB του RPi, και μέσω αυτού δίνεται ρεύμα και σε οποιοδήποτε Relay Module συνδεθεί με αυτό. Για να γίνει αποστολή δεδομένων από το RPi στο Arduino χρησιμοποιείται η σειριακή θύρα (Serial Port) του Arduino.



Εικόνα 2.2: Arduino Uno Rev3, oomlout (2015), Flickr, CC BY-SA 2.0

2.3.4 Λοιπό Hardware

Προκειμένου να συναρμολογηθεί η κατασκευή θα χρειαστουν κάποια συγκεκριμένα υλικά.

Κουτί Κατασκευής (Project Box)

Ανάλογα τον τρόπο σύνδεσης που θα χρησιμοποιηθεί για την σύνδεση του RPi με το Relay Module, και ανάλογα με το αν είναι συμβατό το Relay Module με λογική 3.3V, θα χρειαστεί διαφορετικό μέγεθος κουτιού κατασκευής.

Σύνδεση χωρίς χρήση Arduino: Ο προεπιλεγμένος τρόπος σύνδεσης, από την έκδοση 0.3.1 και μετά είναι χωρίς την χρήση Arduino. Έπειτα από μετρήσεις βρέθηκε οτι το κατάλληλο κουτί κατασκευής έχει διαστάσεις 10cm x 10cm.

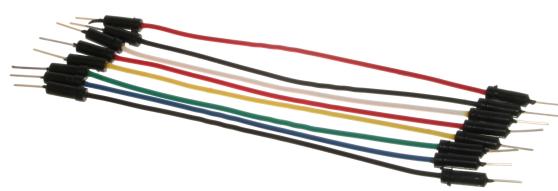
Σύνδεση με Arduino: Εφόσον χρειάζεται να γίνει σύνδεση με Arduino (προκειμένου να μπορεί να λειτουργήσει το Relay Module), έπειτα από μετρήσεις βρέθηκε οτι το κατάλληλο κουτί κατασκευής έχει διαστάσεις 18cm x 14cm.

Καλώδια σύνδεσης

Για να συνδεθεί το Relay Module με το RPi (ή το Arduino), θα χρειαστούν κάποια συγκεκριμένα καλώδια σύνδεσης γνωστά ως Jumper Wires. Τα Jumper Wires κάνουν εύκολη την σύνδεση σε διάφορα εξαρτήματα καθώς δεν χρειάζονται συγκόλληση [7].

Σύνδεση χωρίς χρήση Arduino: Θα χρειαστούν τουλάχιστον 3 Jumper Wires Female-Male (ή Female-Female, σε περίπτωση χρήσης του Male Header).

Σύνδεση με Arduino: Θα χρειαστούν τουλάχιστον 3 Jumper Wires Female-Male, αν χρησιμοποιηθεί Arduino UNO ή 3 τουλάχιστον καλώδια Female-Female, αν χρησιμοποιηθεί Arduino Nano. Επίσης, θα χρειαστεί ένα καλώδιο Micro USB-B to USB-A (OTG Cable) και ένα καλώδιο USB-A to USB-B αν χρησιμοποιηθεί ένα Arduino UNO ή ένα καλώδιο USB-A to Micro USB-B σε περίπτωση χρήσης Arduino Nano.



Εικόνα 2.3: Jumper Wires (Male-Male), oomlout (2009), Flickr, CC BY-SA 2.0

Chapter 3

Συστήματα Ελέγχου Πρόσβασης Πολυκατοικιών/Σπιτιών

Πριν να εξηγήσουμε τον τρόπο κατασκευής και λειτουργίας του PiLock, είναι αναγκαίο να αναφερθούμε στον τρόπο λειτουργίας των περισσότερων κλειδαριών σπιτιών, πολυκατοικιών ή και γραφείων.

Το σύστημα ξεκλειδώματος που χρησιμοποιείται στις περισσότερες κατοικίες αποτελείται από 2 εντελός ξεχωριστά και ανεξάρτητα συστήματα: Το σύστημα του ψυροτηλεφώνου, δηλαδή το σύστημα μέσω του οποίου γίνεται η αναγνώριση του επισκέπτη (μέσω φωνής ή/και εικόνας), και το σύστημα ενεργοποίησης της κλειδαριάς. Στην παρούσα διατριβή θα αναφερθούμε αποκλειστικά στο δεύτερο σύστημα.

Οι ηλεκτρικές κλειδαριές που χρησιμοποιούνται σε πολυκατοικίες συνήθως αποτελούνται από ένα μάνταλο το οποίο, όταν το σύστημα ενεργοποιηθεί μέσω ρεύματος, απελευθερώνεται με αποτέλεσμα να μπορεί ελεύθερα η πόρτα να ανοίξει.



Εικόνα 3.1: Ηλεκτρική κλειδαριά πολυκατοικίας με σύστημα καταγραφής κατάστασης κλειδώματος

Η ενεργοποίηση του παραπάνω συστήματος γίνεται μέσω ενός διακόπτη αναρτημένου πάνω στο ψυροτηλέφωνο του κάθε διαιμερίσματος. Η τροφοδοσία των συστημάτων αυτών μπορεί να γίνεται είτε μέσω απευθείας τροφοδοσίας από το ηλεκτρικό δίκτυο, είτε μέσω κάποιου μετασχηματιστή σε χαμηλότερες τάσεις.

Προκειόντων να μπορέσουμε να ελέγξουμε το σύστημα ξεκλειδώματος, θα πρέπει να μπορέσουμε να βάλουμε έναν δεύτερο διακόπτη, να λειτουργεί παράλληλα με τον

πρώτο.

Chapter 4

Νέος μηχανισμός ξεκλειδώματος

Στο προηγούμενο κεφάλαιο είδαμε από τι αποτελείται ένα σύνηθες σύστημα ξεκλειδώματος πόρτας πολυκατοικίας/σπιτιού. Στο παρόν κεφάλαιο θα αναλύσουμε τον τρόπο σύνδεσης των εξαρτημάτων (βλ 2.3 Υλικό - Hardware), και τον προγραμματισμό τους ώστε να μπορεί να πυροδοτηθεί ξεκλειδωματική πόρτας μέσω υπολογιστή.

4.1 Προετοιμασία του Raspberry Pi

Πρώτο βήμα πριν να γίνει η οποιαδήποτε σύνδεση μεταξύ εξαρτημάτων είναι αναγκαίο να γίνει η εγκατάσταση της τελευταίας έκδοσης του Raspbian Lite στο Raspberry Pi Zero W, καθώς επίσης και να συνδεθεί με το internet. Χρησιμοποιείται η έκδοση Lite έναντι της πλήρης έκδοσης, καθώς δεν χρειάζεται γραφικό περιβάλλον όπως επίσης και τα περισσότερα πακέτα που υπάρχουν προεγκατεστημένα στην πλήρη έκδοση.

Αφότου γίνει η εγκατάσταση του λειτουργικού συστήματος στην κάρτα MicroSD, μπορεί να γίνει η σύνδεση στο Internet είτε Headlessly (χωρίς, δηλαδή, να χρειαστεί να συνδεθεί οιδόνη στο RPi), βάζοντας το αρχείο στο boot partition (διαμέρισμα) της κάρτας μνήμης, και εφαρμόζοντας το παρακάτω configuration, μέσα στο αρχείο `wpa_supplicant.conf`^[8]:

```
1 network={  
2     ssid="YOUR_NETWORK_NAME"  
3     psk="YOUR_PASSWORD"  
4 }
```

Στο πεδίο `ssid` πρέπει να μπει το όνομα του δικτύου στο οποίο πρόκειται να συνδεθεί το RPi. Στο πεδίο PSK πρέπει να γίνει τοποθέτηση του κλειδιού πρόσβασης του δικτύου. Σε περίπτωση που δεν χρησιμοποιείται κρυπτογραφία στο δίκτυο (δεν προτείνεται καθώς μπορεί να συμβεί υποκλοπή δεδομένων από τρίτους), μπορούμε να εισάγουμε το παρακάτω configuration στο ίδιο αρχείο:

```
1 network={  
2     ssid="YOUR_NETWORK_NAME"  
3     key_mgmt=NONE  
4 }
```

Τέλος, πρέπει να γίνει ενεργοποίηση του SSH Daemon στο Raspbian, προκειμένου να είναι εφικτή η απομιακρυσμένη σύνδεση στο RPi, μέσω τοπικού δικτύου. Λόγω

κατασκευής δικτύων bot (botnets) από διάφορους κακόβουλους χρήστες προκειμένου να γίνουν επιθέσεις DDOS (Distributed Denial of Service) από συσκευές Internet of Things που χρησιμοποιούν τα προεπιλεγμένα (default) στοιχεία πρόσβασης (Username, Password), προς διάφορους στόχους, από τον Νοέμβριο του 2016 είναι απενεργοποιημένος εξ' αρχής ο SSH Daemon και πρέπει να ενεργοποιηθεί από τον χρήστη, αν τον χρειάζεται [9]. Για να γίνει αυτό, πρέπει να δημιουργηθεί ένα άδειο αρχείο με το όνομα `ssh` μέσα στο `boot` partition της κάρτας μνήμης του RPi.

Αφότου γίνει η πρώτη εκκίνηση του RPi και βεβαιωθεί οτι υπάρχει ενεργή σύνδεση στο διαδίκτυο, πρέπει να γίνει σύνδεση στο Raspberry Pi μέσω SSH (Username: pi, Password: raspberry) [10].

Προκειμένου να βρεθεί η διεύθυνση IP που χρησιμοποιεί το RPi, ο χρήστης μπορεί να συμβουλευτεί τον πίνακα DHCP του οικιακού Router του, είτε να χρησιμοποιήσει μια εφαρμογή διαγνωστικών δικτύου από κάποιο Smartphone ή H/Y (για Android, και iOS, προτείνεται η εφαρμογή Fing) [13].

Έπειτα, και αφότου γίνει γνωστή η διεύθυνση IP του Raspberry Pi, πρέπει να γίνουν τα ακόλουθα βήματα, προκειμένου να ενημερωθεί πλήρως το Raspbian:

4.1.1 Αλλαγή των προεπιλεγμένων στοιχείων πρόσβασης

Όπως αναφέραμε προηγουμένως, προκειμένου να μην υπάρξει στο μέλλον κίνδυνος επίθεσης, πρέπει να γίνει αλλαγή των προεπιλεγμένων στοιχείων πρόσβασης στο Raspbian. Πρέπει να εκτελεστεί η εντολή `passwd`, και να γίνει εισαγωγή ενός νέου κωδικού πρόσβασης. Ο νέος κωδικός, προκειμένου να είναι ασφαλής, πρέπει να αποτελείται από τουλάχιστον 12 χαρακτήρες, να μην περιέχει μέσα ονόματα, ονόματα από μέρη, ή γενικά λέξεις οι οποίες υπάρχουν μέσα σε λεξικά, και τέλος όταν πρέπει να περιέχει πεζά γράμματα, κεφαλαία, αριθμούς, και σύμβολα [11].

4.1.2 Ενημέρωση του Raspbian

Προκειμένου να εξασφαλιστεί η βέλτιστη λειτουργία και η μέγιστη ασφάλεια στο σύστημα, χρειάζεται να γίνει ενημέρωση των πακέτων του λειτουργικού συστήματος. Πρέπει να γίνει εκτέλεση των επόμενων 2 εντολών [12]:

- 1 `sudo apt-get update`
- 2 `sudo apt-get dist-upgrade`

4.1.3 Ανάθεση στατικής διεύθυνσης IP

Από προεπιλογή, το Raspberry Pi λαμβάνει μια IP διεύθυνση μέσω ενός DHCP εξυπηρετητή στο τοπικό δίκτυο. Αυτή η διεύθυνση IP μπορεί να αλλάξει, μόλις λήξει ο χρόνος μίσθωσης της (DHCP Lease Time). Προκειμένου να λειτουργήσει το PiLock, όταν χρειαστεί η διεύθυνση IP να γίνει στατική, έτσι ώστε να μην αλλάζει.

Αφότου βρεθεί μια διαθέσιμη διεύθυνση IP στο τοπικό δίκτυο (που να είναι εκτός του εύρους διευθύνσεων που να μπορεί να αναθέτει ο DHCP Server), και αφού καταγραφεί και η μάσκα υποδικτύου που αντιστοιχεί στο συγκεκριμένο υποδίκτυο, καθώς επίσης και η διεύθυνση προεπιλεγμένης πύλης, πρέπει να γίνει ανάθεση της συγκεκριμένης διεύθυνσης IP μέσω του DHCP Client Daemon (`dhcpcd`). Για να

γίνει αυτό πρέπει να γίνει επεξεργασία του αρχείου `/etc/dhcpcd.conf` και να γίνει πρόσθεση των παρακάτω γραμμών, στο τέλος του αρχείου:

```
1 interface wlan0
2   static ip_address=192.168.1.2/24
3   static routers=192.168.1.1
4   static domain_name_servers=192.168.1.5
5   static domain_search=home.lan
6   noipv6
```

Στο παραπάνω παράδειγμα, αναθέτουμε την διεύθυνση 192.168.1.2, με μάσκα υποδικτύου την 255.255.255.0 (24 bits μάσκας). Θέτουμε επίσης ως προεπιλεγμένη πύλη (Router) την συσκευή με την διεύθυνση 192.168.1.1 και ως διακομιστή DNS την συσκευή 192.168.1.5. Προαιρετικά, μπορούμε να θέσουμε και το Search Domain. Σε αυτό το παράδειγμα το θέτουμε σε home.lan. Με την τελευταία γραμμή, υποχρεώνουμε το DHCPCD να απενεργοποιηθεί, για διευθύνσεις IPv6.

Αφότου γίνει η αλλαγή των προεπιλεγμένων στοιχείων πρόσβασης και η ενημέρωση του συστήματος, πρέπει να απενεργοποιηθεί το σύστημα προκειμένου να συνδεθεί με το Relay.

4.2 Σύνδεση με το Relay

Για να γίνει η σύνδεση του Raspberry Pi με το Relay, πρέπει να επιλέξουμε έναν από τους 2 τρόπους σύνδεσης, ανάλογα με τη Relay Module όπου χρησιμοποιηθεί (βλ. 2.3.2 Relay Module).

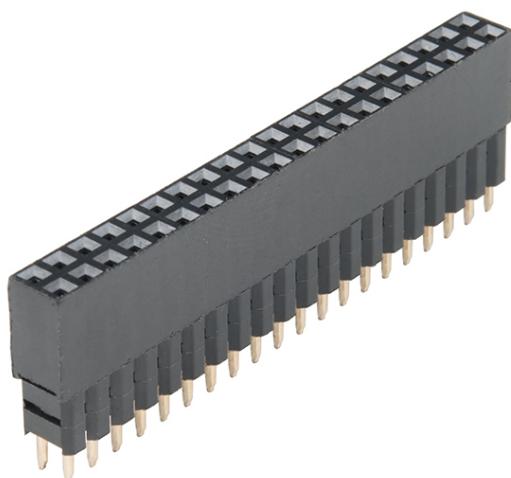
4.2.1 Σύνδεση χωρίς την χρήση Arduino

Προκειμένου να γίνει σύνδεση του RPi με το Relay Module, όπου χρειαστεί να κολληθούν κεφαλές υποδοχής για Jumper Wires στα GPIO του Raspberry Pi. Μπορούν να χρησιμοποιηθούν είτε Female, είτε Male τύπου Headers, αλλά από αυτό όταν εξαρτηθεί τι Jumper Wires όπου χρειαστούν για να συνδεθεί το RPi με το Relay Module (Male-Female αν χρησιμοποιηθεί Female Header, Female-Female αν χρησιμοποιηθεί Male Header).

Αφότου γίνει η κόλληση των Headers, μπορούν να χρησιμοποιηθούν τα αντίστοιχα καλώδια προκειμένου να συνδεθεί το Relay Module. Πρέπει ο χρήστης που όταν συνδέεται να συμβουλευτεί το διάγραμμα των GPIO Pins (γνωστό ως Pinout). Στο συγκεκριμένο παράδειγμα (Εικόνα 4.2), έχει συνδεθεί στο GPIO Pin 18 (πράσινο καλώδιο). Για παροχή ρεύματος χρησιμοποιείται το 3V3 Pin (κόκκινο καλώδιο) και για Ground χρησιμοποιείται ένα από όλα τα GND Pins (μαύρο καλώδιο).

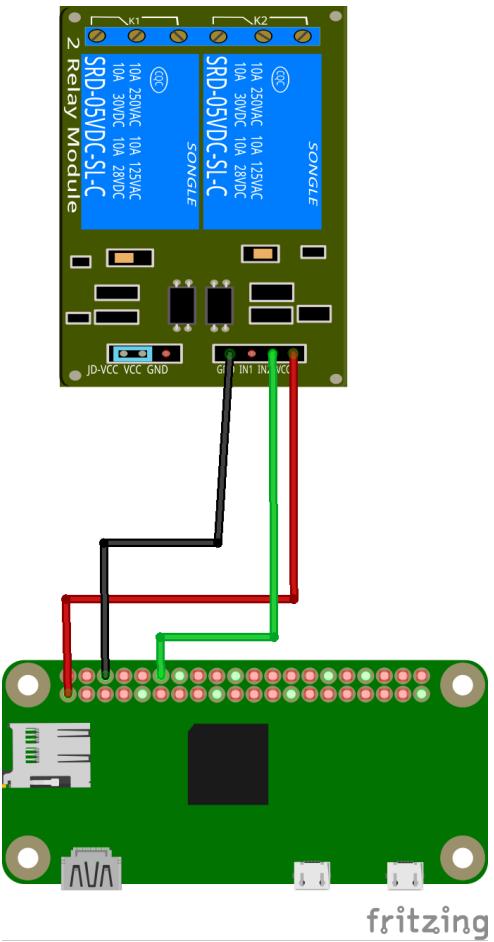
4.2.2 Σύνδεση με την χρήση Arduino

Αφότου γίνει Upload το Arduino Script που χρειάζεται για την λειτουργία του PiLock (βλ. ?? ??), μπορεί να γίνει σύνδεση του Arduino με το Relay. To Relay Board μπορεί να συνδεθεί σε ένα από όλα τα Digital Pins του Arduino (πράσινο καλώδιο) (Εικόνα 4.3). Ρεύμα δίνεται μέσω του 5V Power Pin του Arduino και το Ground συνδέεται σε ένα εκ των τριών GND Pins του Arduino.

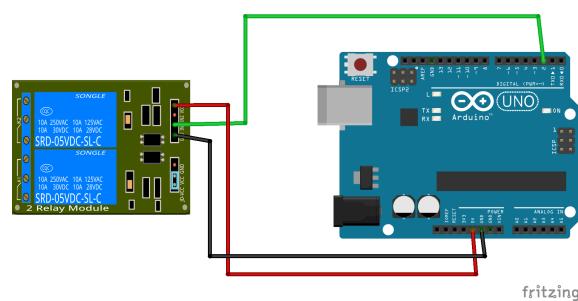


Εικόνα 4.1: Female GPIO Headers, SparkFun Electronics (2016), Flickr, CC-BY 2.0

Αφότου συνδεθεί το Relay Module με το Arduino, πρέπει να συνδεθεί το Arduino με το Raspberry Pi. Αυτό γίνεται συνδέοντας το καλώδιο OTG (βλ. 2.3.4 Σύνδεση με Arduino:) με το RPi, και την άλλη άκρη του με το Καλώδιο USB του Arduino.



Εικόνα 4.2: Σύνδεση ενός Raspberry Pi Zero W με ένα Relay Module



Εικόνα 4.3: Σύνδεση ενός Arduino με ένα Relay Module.

Chapter 5

Προγραμματιστικό Περιβάλλον - Τεχνολογίες που χρησιμοποιήθηκαν

Στο παρόν κεφάλαιο θα αναφερθούμε στα εργαλεία που χρησιμοποιήθηκαν κατά την ανάπτυξη του PiLock, καθώς επίσης και στον τρόπο διαχείρησης του έργου ανάπτυξης.

5.1 Η σημασία χρήσης δωρεάν λογισμικού ανοικτού κώδικα κατά την ανάπτυξη του PiLock

Ος ”Λογισμικό Ανοικτού Κώδικα” (Open Source Software) ορίζεται το λογισμικό του οποίου ο πηγαίος κώδικας είναι διαθέσιμος ελεύθερα προς το κοινό προκειμένου να μπορεί να τροποποιηθεί, να αναβαθμιστεί ή να μελετηθεί. Ο πηγαίος κώδικας, για τον απλό χρήστη είναι ένα τμήμα του λογισμικού που δεν έχει δει ποτέ. Σε έργα ανοικτού κώδικα, μπορεί ο οποιοσδήποτε να προτείνει διορθώσεις, αναβαθμίσεις ή προσθήκη χαρακτηριστικών^[14].

Εξαιτίας αυτού του χαρακτηριστικού, και των αδειών που το υποστηρίζουν, το λογισμικό ανοικτού κώδικα μπορεί να χρησιμοποιηθεί για οποιοδήποτε σκοπό επιθυμεί ο χρήστης, χωρίς να περιορίζεται από κάποια άδεια χρήσης. Επίσης, παρέχει αυξημένη ασφάλεια, εφόσον μπορεί να δοκιμαστεί και να μελετηθεί από τους προγραμματιστές ο πηγαίος κώδικας του. Στο λογισμικό κλειστού κώδικα, είναι αδύνατον να μελετηθεί και να τροποποιηθεί από τρίτους ο κώδικας του, και κατ’ επέκταση, εφόσον υπάρξει ένα κενό ασφαλείας θα πάρει συνήθως αρκετά περισσότερο χρόνο μέχρι να κυκλοφορήσει μια ενημέρωση ασφαλείας. Τέλος, εξαιτίας της ευελιξίας που παρέχει, το λογισμικό ανοικτού κώδικα μπορεί να τροποποιηθεί προκειμένου να μπορέσει καλύτερα να καλύψει τις ανάγκες του χρήστη^{[14], [15]}.

Μία υποκατηγορία του λογισμικού ανοικτού κώδικα είναι το **Δωρεάν Λογισμικό Ανοικτού Κώδικα** (Free and Open Source Software, FOSS), το οποίο επιτρέπει στον χρήστη να το κατεβάσει και να το χρησιμοποιήσει χωρίς κάποιο κόστος. Το λογισμικό που χρησιμοποιήθηκε για την ανάπτυξη του PiLock ανήκει στην κατηγορία αυτή.

5.2 Version Control

Καθ' όλη την διαδικασία ανάπτυξης του PiLock χρησιμοποιήθηκε σύστημα Version Control. Τα Συστήματα Version Control βοηθούν τον/τους προγραμματιστή/ές καθώς προσδίδουν ασφάλεια και ευελιξία κατά την ανάπτυξη και την συντήρηση ενός έργου. Το Git είναι το λογισμικό Version Control που χρησιμοποιήθηκε κατά την ανάπτυξη του PiLock.

Το Git δημιουργήθηκε από τον Linus Torvalds το 2005 προκειμένου να τον βοηθήσει στην ανάπτυξη του Linux Kernel. Διάφοροι άλλοι συνεισφέροντες προς το Linux Kernel βοήθησαν στην ανάπτυξη του Git, κατά την πρώτη περίοδο της ανάπτυξης του. Αποτελεί δωρεάν λογισμικό ανοικτού κώδικα και διανείμεται υπό την άδεια GNU General Public Licence, έκδοση 2.

Πιο συγκεκριμένα, εξαιτίας της ικανότητάς του Git να διατηρεί ιστορικό για όλα τα αρχεία ενός έργου, το έργο μπορεί να επανέλθει σε μία προηγούμενη κατάστασή του, ανά πάσα στιγμή. Οι "καταστάσεις" είναι γνωστές ως "Commits". Με αυτό τον τρόπο, δεν απορρίπτεται κώδικας, πολλές φορές πολύτιμος για την ανάπτυξη ενός έργου. Επίσης, μέσω του σύστημα staging του Git, ο προγραμματιστής γνωρίζει τι ακριβώς κρατείται σε ένα νέο Commit, όποτε καταχωρηθεί. Με το branching system του Git, καθίσταται δυνατόν να τροποποιείται ή να προστίθεται κώδικας και νέα features χωρίς να τροποποιείται ο Stable κώδικας του έργου (για παράδειγμα, το κάθε release χρησιμοποιεί υποχρεωτικά νέο branch), ο οποίος "ενημερώνεται" στο τέλος του κάθε release/feature, προκειμένου να αποφευχθούν προβλήματα. Τέλος, το Git διευκολύνει σημαντικά την συνεργασία μεταξύ προγραμματιστών καθώς μπορεί ο κάθε προγραμματιστής να δουλεύει το δικό του "κομμάτι" κώδικα, χωρίς να επηρεάζει την πρόοδο των υπόλοιπων προγραμματιστών που δουλεύουν πάνω στο έργο.

Στην ανάπτυξη του PiLock, το λογισμικό της πλευράς του Εξυπηρετητή, του Πελάτη καθώς επίσης και τα σενάρια ξεκλειδώματος (Unlock Scripts) διαχειρίζονται ξεχωριστά σε διαφορετικά αποθετήρια. Συγκεκριμένα, τα σενάρια ξεκλειδώματος αποτελούν submodule του λογισμικού του εξυπηρετητή.

Προκειμένου να γίνει σωστή διαχείρηση της διαδικασίας ανάπτυξης, ακολουθήθηκαν κάποιοι κανόνες. Οι κανόνες αυτοί διασφαλίζουν την ακαιρεότητα του κώδικα ανα πάσα στιγμή κατά την ανάπτυξη. Πιο συγκεκριμένα:

- Η σταθερή (Stable) έκδοση του κώδικα βρίσκεται στο master branch.
- Όποια αλλαγή πρόκειται να γίνει στον κώδικα, είτε αυτή είναι hotfix, είτε κάποιο νέο feature, είτε documentation, θα πρέπει να γίνεται αποκλειστικά σε νέο branch με χαρακτηριστικό τίτλο, ο οποίος να ξεκινά από το ανάλογο prefix. Συγκεκριμένα, αν πρόκειται για νέο feature να χρησιμοποιεί το "feature" prefix, αν πρόκειται για bugfix να χρησιμοποιεί το "bug" ή το "hotfix" prefix, και αν πρόκειται για αλλαγή στο documentation ή στο Readme, να χρησιμοποιεί το "doc" prefix. (Πχ. feature/pin-changing)
- Τα νέα Branches, εφόσον ελεγχθούν, θα πρέπει να συγχωνεύονται στο αντίστοιχο branch στο οποίο απευθύνονται (βλ. παρακάτω).
- Νέα λειτουργικότητα (νέα features) προστίθεται μόνο στα νέα releases (στο branch του εκάστοτε νέου release). Τα hotfix καθώς επίσης και διάφορα bugs μπορούν να συγχωνεύονται απευθείας με το master, αρκεί να έχουν ελεγχθεί εξονυχιστικά πρώτα και να είναι υψηλής προτεραιότητας.

- To master branch, καθώς επίσης και τα branches για νέα releases θα πρέπει να είναι κλειδωμένα και να δέχονται συγχονεύσεις μόνο εφόσον περάσει από έγκριση ο κώδικας μέσω κάποιου Pull Request ή Merge Request.

Αρχικά, μέχρι την πρώτη δημόσια έκδοσή του (0.2.0), ο κώδικας του PiLock φιλοξενούνταν στον προσωπικό εξυπηρετητή του δημιουργού, και διαχειρίζονταν τα αποθετήρια του μέσω του δωρεάν λογισμικού διαχείρησης αποθετηρίων Git γνωστό ως GitLab (<https://about.gitlab.com>). Αργότερα, από την πρώτη δημόσια έκδοσή του PiLock και μετά, ξεκίνησε να χρησιμοποιείται το GitHub (<https://github.com>) ως χώρος φιλοξενίας του έργου και των αποθετηρίων του.

Bibliography

- [1] Kevin Ashton (2009), "That 'Internet of Things' thing"
<http://www.rfidjournal.com/articles/view?4986>
- [2] Jim Hill (2015), "The smart home: a glossary guide for the perplexed"
<https://www.t3.com/features/the-smart-home-guide>
- [3] Ian Paul (2017), "The \$10 Raspberry Pi Zero W brings Wi-Fi and Bluetooth to the minuscule micro-PC"
<https://www.pcworld.com/article/3175256/computers/the-10-raspberry-pi-zero-w-brings-wi-fi-and-bluetooth-to-the-minuscule-micro-pc.html>
- [4] Eben Upton (2015), "RASPBERRY PI ZERO: THE \$5 COMPUTER"
<https://www.raspberrypi.org/blog/raspberry-pi-zero/>
- [5] Relay, Wikipedia
<https://en.wikipedia.org/wiki/Relay>
- [6] Arduino for Beginners, Makerspaces.com
<https://www.makerspaces.com/arduino-uno-tutorial-beginners/>
- [7] Jump Wire Structure (2003), Katayama Tatsuo
<http://www.freepatentsonline.com/6899560.html>
- [8] How to connect raspberry pi to WiFi without a monitor (2017), Chetan Kapoor
<https://installvirtual.com/how-to-connect-raspberry-pi-to-wifi-without-a-monitor>
- [9] A security update for Raspbian PIXEL (2016), Simon Long
<https://www.raspberrypi.org/blog/a-security-update-for-raspbian-pixel/>
- [10] <https://www.raspberrypi.org/documentation/linux/usage/users.md>
- [11] How to Create a Secure Password You Can Remember Later: 4 Key Methods (2014), Kevan Lee
<https://open.buffer.com/creating-a-secure-password/>
- [12] Updating and Upgrading Raspbian <https://www.raspberrypi.org/documentation/raspbian/updating.md>
- [13] <https://www.raspberrypi.org/documentation/remote-access/ip-address.md>

- [14] Τι είναι το λογισμικό ανοικτού κώδικα: Μια εισαγωγή (2015), Κώστας Παπαδήμας
<https://ellak.gr/2015/09/ti-ine-to-logismiko-aniktou-kodika-mia-isagogi/>
- [15] 10 Reasons Open Source Is Good for Business (2010), Katherine Noyes
https://www.pcworld.com/article/209891/10_reasons_open_source_is_good_for_business.html