<UNDECIDABLES>

COSBAS User Manual

Git: `https://github.com/undecidables/Documentation`
GitHub Organisation: `https://github.com/undecidables`

The Team:
Elzahn Botha *13033922*
Jason Richard Evans *13032608*
Renette Ros *13007557*
Szymon Ziolkowski *12007367*
Tienie Pritchard *12056741*
Vivian Venter *13238435*

August 2015

Contents

1 Introduction

The COSBAS system is a highly secure and modern access control system that uses Biometric data to authorize the individuals request to enter the department and offices. This document will specify how to place the COSBAS system in a working state. The document instructs on the necessary steps to install the hardware needed by our system as well as installing the COSBAS system software on the relevant computers.

2 System Overview

2.1 Overview Description:

The COSBAS (Computer Science Biometric Access System) is a secure system that uses Biometric inputs (such as facial recognition and fingerprint scanning) to unlock and gain access to the department and offices.

2.2 Pinpoint Descriptions:

2.2.1 COSBAS-Client

The COSBAS client is the hardware aspect of the COSBAS system. It will allow users to capture biometric data to be used as authentication for access to the department. The images are taken (be it facial, fingerprint etc.) and then sent off to the server for authentication while waiting for a response from the server to permit the access or not. Initally the COSBAS system will only have the functionality of Facial Recognition and Fingerprint Identification. With facial recognition, a set of images are take but only the images with the most centered face is sent to the server for authentication purposes. If no face is detected, then the user would have to retry the process. Fingerprint images are close proximity images and hence will always be accurate enough to send it directly to the server for authentication.

2.2.2 Web-Client

The interface for the COSBAS system will be a responsive webpage the user (authorized and temporary visitors) may use to request permission for access to the department. They can also book appointments with members of faculty on the system.

2.2.3 Bookings and Appointments

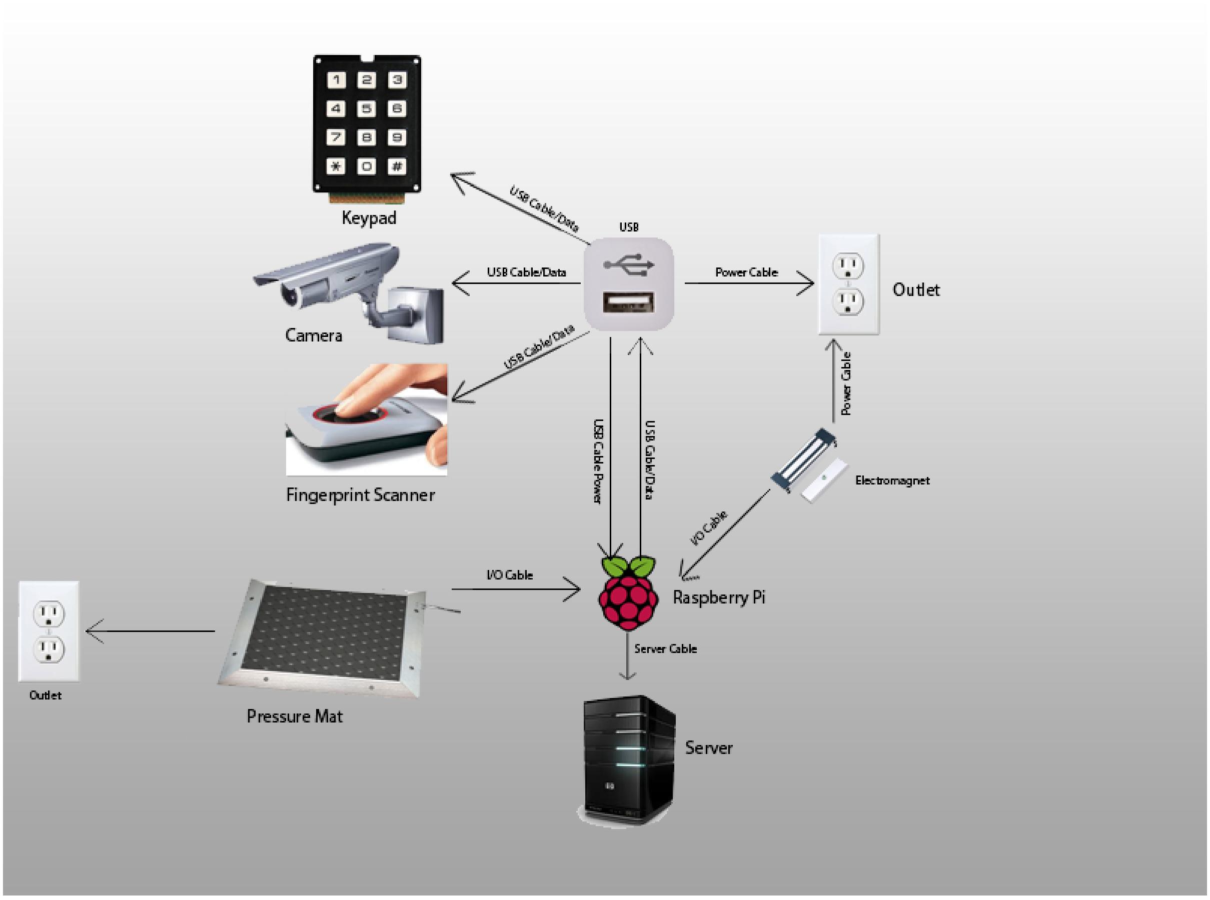
An unothorized user can book an appointment with an employee enrolled in the system by making use of a Calendar integration feature on the web based interface. Authorized users can then either accept or decline the booking for an appointment of which the person whom made the booking is notified of the status of their booking via an email.

2.2.4 Temporary Access

Once a booking has been accepted by the authorized user of COSBAS, they will be notified via email containing a link that will expose their temporary access code generated by the COSBAS system. There will also be another link in the email the user may click on to cancel the appointment with the associated COSBAS user. In such a case, the temporary access code will be revoked.

3 System Configuration

3.1 Graphical System Configuration diagram



3.2 Description of the equipment used as illustrated on the diagram

- Client - Raspberry PI: Is a very small computer with a very low power consumption. The PI can handle quite a few input/ouput devices via the USB/HDMI/LAN/GPIO ports
- Camera: A device which will capture an image of the user that will want to authenicate via biometrics.
- Fingerprint scanner: A device that will caputer the finger print of the user which will be used for authentication.
- Keypad: Will be used by users that will gain access to the building via the keycode.
- USB Hub: This device will allow us to connect more than one device via USB to the client as well as give power to the client.
- Pressure mat: This device will allow us to pick up that the user is ready to be authenticated to gain access to the building.

- Electromagnet door lock: Will keep the door locked until the client has succesfully authenticated the user.
- Server: Will be used for all the heavy computations such as facial/finger print recognition, etc.

3.3 System Configuration Explained

The system is made up of pluggable authentication devices such as a keypad, camera and fingerprint scanner, as well a client (Raspberry Pi) and a server. The entire authentication process is started a soon as the user steps onto the pressure mat sending the authentication data to the Raspberry Pi for processing before it is sent to the server for authentication. Once authentication is complete on the server, a reply will be sent to the client and the client will act accordingly.

3.4 Communication and networking

The pressure mat, USB Hub and electromagnet door lock all get their power from the main outlet while the keypad, camera and fingerprint scanner will be getting their power via the USB connection. The Raspberry Pi also connects to the USB Hub both for power and data transfer between the authentication devices and the client. The client communicates with the server via a LAN cable and the pressure mat and electromagnet door lock connects to the client GPIO pins via I/O cables.

Once the user steps onto the pressure mat a signal is sent to the client which gets its data from the authentication devices and processes that data before sending it off to the server if it was valid data. The server the authenticates the person and sends the data back to the client that will then, if the authentication was successful, open the door for the user.

4 Installation of the COSBAS System

5 Getting Started

6 Using the System

7 Troubleshooting