Sistema de seguridad biométrico mediante sensor de huellas dactilares para la apertura de puertas del centro de datos de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia

Perfil de proyecto de grado para la obtención del titulo de Ingeniero Electrónico de la Facultad de Ingeniería otorgado por la Universidad Mayor de San Andrés

Autor: Daniel Jiménez Jerez

2015

Índice

1. Introducción

El presente documento propone un perfil de proyecto de grado, el cual trata del diseño de un sistema de seguridad para la apertura de puertas mediante el uso de huellas dactilares, mismas que son reconocidas mediante sensores que se comunican con un servidor que determina la apertura de las puertas de acuerdo a los registros de huellas y permisos contenidos en una base de datos.

Durante el desarrollo del proyecto se diseñarán los programas necesarios para la transferencia de paquetes de datos desde cada uno de los sensores hasta el servidor que contiene la base de datos. Para este fin se propone el uso de Arduino[1], por su capacidad de procesamiento, transmisión fiable de datos y sobre todo por su gran flexibilidad para poder realizar con mayor facilidad futuras mejoras del proyecto.

Dada la naturaleza de los ambientes que se intenta resguardar, se debe tomar muy en cuenta la seguridad durante cada tramo que recorren los datos, es por ello que se diseñarán protocolos de intercambio de datos que contendrán una cabecera robusta con varios niveles de verificación, todo esto para evitar en lo posible la corrupción de datos, intentos de acceso por fuerza bruta y/o errores en los paquetes de datos.

En cuanto al servidor, se propone el uso de un Raspberry[2] ya que cuenta con los el hardware y software necesario para este trabajo. Este ordenador actuara como un servidor de bases de datos y a la vez como servidor web.

El diseño de la interfaz de administración y los programas de comunicación del lado del servidor se implementaran en el entorno Python[3].

El lenguaje de programación de Arduino esta basado en C pero contiene aditivos, librerías propias de Arduino que incrementan brindan acceso a las diferentes funcionalidades del hardware, de esta adición proviene el lenguaje Processing[4].

Por ultimo la base de datos propuesta se implementara en PostgreSQL[5].

Como se puede apreciar se intenta utilizar en lo posible tanto software como hardware libre durante todo el desarrollo del proyecto.

[1] Plataforma de hardware libre basada en los microcontroladores Atmel AVR
[2] Ordenador de placa reducida de bajo coste
[3] Lenguaje de programación multiplataforma con tipado dinámico
[4] Entorno de desarrollo integrado de código abierto basado en Java
[5] Sistema de gestión de bases de datos relacional orientado a objetos

2. Planteamiento del problema

El termino seguridad proviene del latín *securitas* y se usa para definir el concepto de algo donde no se registran peligros, daños ni riesgos. Una cosa segura es algo firme, cierto e indubitable. La seguridad , por lo tanto, puede considerarse como una certeza. Desde la prehistoria el hombre ha tratado de buscar seguridad en diferentes ámbitos de su diario vivir, desde tratar de encontrar un refugio donde se sienta a salvo de las inclemencias de la naturaleza, pasando por los candados con los que se impide el acceso a personas no autorizadas, hasta las bóvedas que resguardan dinero o información confidencial.

En particular la seguridad informática permite asegurar que los recursos del sistema se utilizan de la manera en la que se espera y que quienes puedan acceder a la información en el que se encuentran sean las personas acreditadas para hacerlo.

En la rama informática existen dos tipos de seguridad:

- La seguridad física que impone barreras físicas para impedir el paso al sistema de cualquier persona no acreditada mediante habilidades propias del ser humano como ser la firma o las contraseñas, o mediante características del cuerpo humano como ser el iris del ojo, la forma del rostro o las huellas dactilares, y aspectos que diferencian a un ser humano de otro, que se repiten o duplican en muy bajo porcentaje.

- La seguridad lógica que trabaja sobre el encriptado y desencriptado de códigos para que no pueda ser legible por personas que no conozcan el método de encriptación, y la fiabilidad de los datos que garantizan el proceso de comunicación y brindan a su vez una medida mucho menor de los errores que se producen durante el trayecto.

Entonces al trabajar con la seguridad de un recinto, se elabora un sistema de prevención en caso de complicaciones, desastres y principalmente se trata de imponer barreras para que solo personas autorizadas tengan acceso a dicho recinto.

Es aquí donde recae la problemática, que se genera en base a todos los conceptos anteriores y que trata el tema de: ¿como brindar seguridad para el ingreso al recinto que se quiere resguardar?

3. Justificación

En la actualidad de pueden encontrar sistemas de seguridad que contienen uno o varios métodos de identificación de personas, a pesar de ello se puede verificar que tanto el software como el hardware de estos sistemas son propietarios, es decir no se puede modificar o alterar el funcionamiento ni del software ni del hardware, solo se puede hacer uso de estos sistemas con todas las privaciones que conllevan. Es por ello que se intenta diseñar un sistema que es a medida pero que a su vez sea flexible a modificaciones, alteraciones o mejoras y que se base en el mismo concepto de seguridad que los sistemas actuales.

Este proyecto esta basado en hardware existente, de bajo costo, de desarrollo comunitario, es decir que se tienen licencias de uso y reproducción total y/o parcial, además también se utiliza software de código abierto que tiene las mismas características de uso y reproducción que vienen tipificadas mediante diferentes licencias como ser GNU, BSD, Apache, etc.

El propósito del presente proyecto es el de aplicar los conocimientos adquiridos durante la carrera de Ingeniería Electrónica en cuanto a las materias de bases de datos, ingeniería de software y la interacción entre hardware/software para poder diseñar un sistema de seguridad que brinde el acceso a personas autorizadas a recintos restringidos, tanto en lo que se refiere a la parte física, que incumbe la conexión desde un sensor de huellas dactilares hasta un servidor, y desde el servidor hasta la puerta de ingreso al recinto, así como también el sistema gestor de bases de datos y el sistema de administración, a su vez se diseñaran protocolos de comunicación para evitar el mayor numero de errores que puedan generarse y brindar un alto grado confiabilidad y robustez al sistema.

Es por todo lo anterior que este proyecto brinda un aporte de valor técnico-científico al observar la originalidad del diseño y los medios que se utilizaran para realizarlo que a su vez conllevan una cuantiosa reducción del costo monetario en comparación con los sistemas que se pueden encontrar en el mercado.

4. Objetivos

4.1. Objetivo general

- Diseñar un sistema de seguridad robusto y fiable para el ingreso al centro de datos de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia mediante el uso de sensores biométricos de huella dactilar en conjunción con el proceso de comparación de un servidor de bases de datos, basado en la medotodolgía de hardware y software libre.

4.2. Objetivos específicos

- Diseñar los sistemas de interconexion fisica para lograr una comunicacion fiable y segura.
- Elaborar un sistema de protocolos de comunicacion robusto con diferentes grados de verificacion tanto para la transmision como para la recepcion de los datos en cada trayecto en el que estos viajen.
- Construir una interfaz de usuario amigable para la administracion e inscripcion de personas al sistema propuesto.
- Utilizar hardware libre tanto para el servidor como para las conexiones tipo puente que se necesitan para llegar desde y hacia los sensores.
- Programar el sistema gestor de bases de datos, el sistema de administracion y los programas que reciben y envian datos desde y hacia los sensores y puertas utilizando software libre.
- Reducir el costo economico en software y hardware tomando como referencia los sistemas de seguridad que se encuentran disponibles en el mercado.

5. Marco teórico